First Edition, May 2020

The DG Data Trends Report

Assessing the Risk of Data Loss During the COVID-19 Pandemic

Introduction from Tim Bandos Vice President, Cybersecurity

For employers, COVID-19 has dramatically heightened the risk of data loss.

On March 11, 2020 the World Health Organization (WHO) declared COVID-19 a global pandemic. Within days, organizations all over the globe instantly transformed themselves into distributed companies with 100% of their employees working from home. This remote work dynamic, combined with the fact that very few employees were trained on how to securely work from home, has created a perfect storm for sensitive data loss.

The economic impacts of COVID-19 are also being felt around the world and we already know how economic turmoil can fuel data loss. The most egregious example, the financial crisis of 2007-2009, led to 37 million unemployment claims. It also resulted in a slew of trade secret theft charges. In 2013, the Department of Justice said it charged more than 1,000 defendants with intellectual property theft between 2008 and 2012.

Tim Bandos
VP, Cybersecurity
Digital Guardian

Many of those employees left companies and either got jobs with competitors or started their own companies with stolen data. As of late-May 2020, over 38.6 million Americans have filed for unemployment, leaving many of those still employed feeling uncertain about their own job stability. Whether we see the same levels of IP theft to follow this crisis remains to be seen.

Another consideration, and more likely in today's work from home environment, is the loss of sensitive data due to well-meaning employees simply looking for ways to get their jobs done. In many scenarios, employees with access to highly sensitive data are working from home with less access to corporate network data shares and sanctioned collaboration tools. While the risks around data leakage have always loomed large over companies, employees working from home during a global pandemic has only further exacerbated them.

To quantify the true scope of risk introduced by COVID-19, we looked at data movement activity at 194 companies using the Digital Guardian Data Protection Platform before and after the COVID-19 global pandemic declaration.

Unlike other "data risk reports" that are based on survey data, this report is based on real data from organizations spanning the globe and across multiple industry verticals. Our unique classification and data visibility capabilities allow us to share how much data was egressed, and whether or not the data was classified.

We hope this report is a useful resource to assist your organization in understanding and mitigating your organization's data loss risk during the COVID-19 pandemic and beyond.

– tim

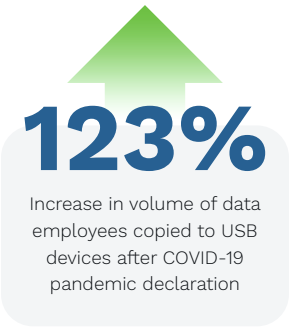
Summary of Findings

Risk to sensitive data from both insider and outsider threats has spiked since the WHO declared the COVID-19 outbreak a global pandemic on March 11, 2020. Almost overnight, thousands of companies around the world were forced to transform into distributed organizations where working from home is the "new normal." Many organizations were not prepared for this transition. This has introduced a significant increase in the risk of sensitive data loss as remote employees move and use data via unsanctioned means. The risks to sensitive data have been compounded by external adversaries, trying to take advantage of the new work from home phenomena through increased opportunistic attacks on remote workers.

Key Takeaways

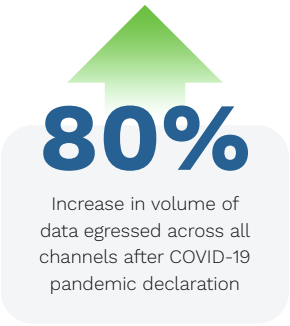
After the COVID-19 pandemic declaration, employees are storing much larger volumes of sensitive data on USB devices.

Since the onset of COVID-19, we have seen a **123%** increase in the volume of data moving to USB drives and **74%** of that data was classified according to the DLP policies. USB devices are a common vehicle for sharing data and we regularly see employees in offices download large files to USB devices and drop them off at a co-worker's desk to collaborate on content. However, with most states and countries under stay-at-home and shelter-in-place orders, "handing off" a physical USB device to a co-worker or trusted partner is practically impossible. Given that, we would have assumed the data would show a decrease in USB usage after COVID-19. Instead, we've seen a dramatic increase. While it's difficult to attribute employee motives for this behavior, we can confirm the behavior exists and that organizations should take heed.



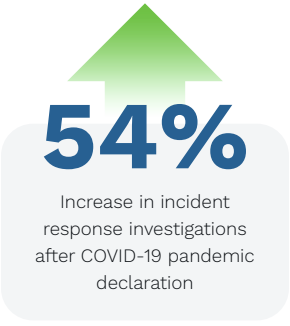
Data egress has spiked across the board. Security teams thinking a return to the office (with the requisite network protections) is imminent must think again.

With employees working from their homes, data egress via all means (email, cloud, USB, etc.) was **80%** higher in the first month following WHO's COVID-19 pandemic declaration. More than **50%** of observed data egress was classified data. Executives who believe returning to the office and its security protections will return them to an acceptable risk level must think again. Many global healthcare and government leaders now accept that the effects of COVID-19 will be with us for the foreseeable future. Working from home will be the rule, not the exception. This should increase the urgency for executives and security teams who oversee a remote workforce to prioritize data protection vs. waiting to get back to the office and simply hoping to avoid data loss until that time.



Organizations should enlist every employee in their battle to protect sensitive data and IP from outside attackers.

The global cybersecurity talent shortage is well-documented. In-house security teams were taxed well before the onset of a global pandemic but COVID-19 has impaired the situation further. Digital Guardian's Managed Detection & Response customers have noticed a **62%** increase in malicious activity, a number that in turn has led to an increase in incident response investigations – **54%** more than before the WHO's pandemic declaration. The best option to expand your security team today is to enlist every employee to be a part of the effort. Organizations should continue to offer security awareness training to keep their first line of defense strong. Training can also make it less likely that low-level attacks, like phishing, put sensitive data at risk.



Increased Volume of Corporate Data Egressed by Egress Path After COVID-19

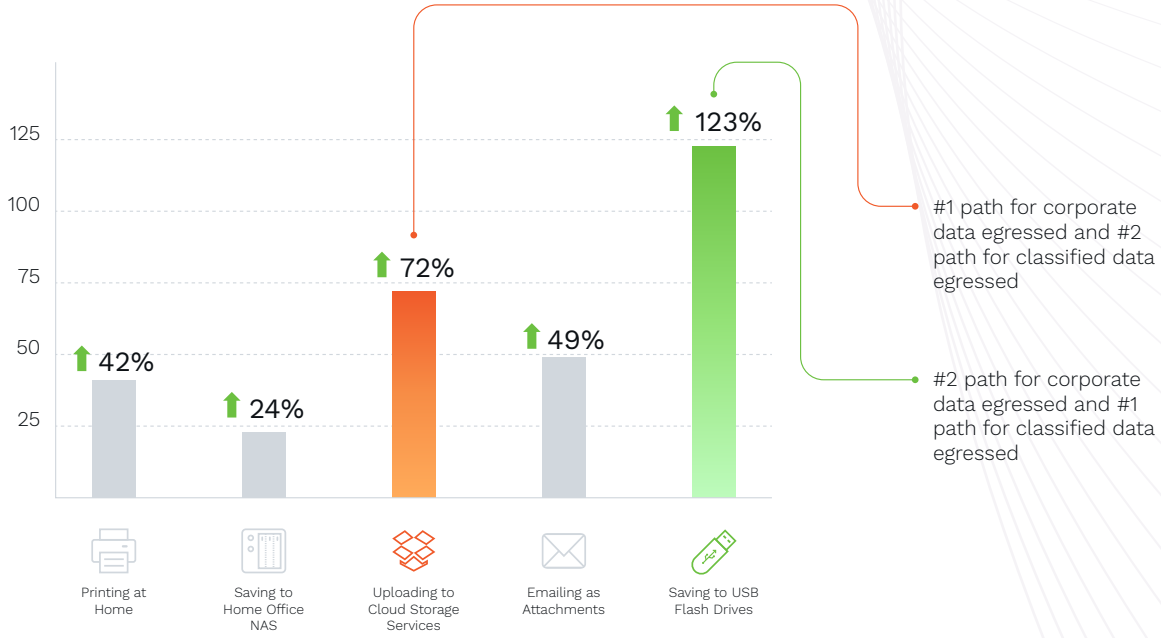


FIG 1. *Increased Volume of Corporate Data at Risk*
Source: *The DG Data Trends Report by Digital Guardian*

One of the report's most important findings highlights the risk inherent in USB devices, they remain one of the most popular ways to store and transport files from one computer to another.

Since the WHO declared the outbreak a pandemic, we observed a **123%** increase in the volume of data employees are copying to USB devices. With so many employees across the world under shelter-at-home orders, it seems unlikely that employees are using a USB device to share files or collaborate with co-workers. How are employees handing the device to a co-worker? This statistic may suggest workers in fear of losing their job during this crisis are storing data to give them a leg up at a new job or to use later in their career. Even if this is not the case, duplicating data on USB devices increases the volume of data that can be lost or stolen. The portability of USB drives also means they can be misplaced.

When it comes to cloud file sharing sites, our data found that there's been a spike in the volume of data employees are uploading to services like Box, Dropbox, and Google Drive.

If an organization doesn't have a solution in place to mitigate data loss, cloud storage providers can act as an easy avenue for employees to egress sensitive data. While many companies prohibit employees from storing confidential data in non-sanctioned cloud storage services like iCloud, Google Drive, and Dropbox, not every company has the technology to see and outright block the activity. While accessing these services might be restricted in the office, that may not be the case for employees while working at home. Depending on their configuration, layered controls, like proxy servers and firewalls, may not be enforced while off-network.

It's not just cloud storage apps; employees are going the old-fashioned route too, sending sensitive data via email. Our data shows a **47%** uptick in sensitive data being sent via email. In lieu of copying data to a USB drive or a cloud drive, it's an unfortunate reality that some employees may be sending sensitive files – Excel sheets, PowerPoint slide decks, etc. - as attachments in emails to their personal email, further increasing its risk of loss.

Other methods of data egress included home printer devices (38%) and personal network-attached storage devices (24%).

Data Egress by Volume Before and After COVID-19 Pandemic Declaration

	Avg. Monthly Data Egress (TB) Jan - Feb 2020	Avg. Monthly Data Egress (TB) Mar - Apr 2020	Avg. Monthly Data Egress Change (+/-)
USB Drives	99	221	+123.2%
Cloud Storage Services	195	336	+72.3%
Email	7	10.4	+48.6%
Printer	1.9	2.7	+42.1%
NAS	46	57	+23.9%
Data Egress	**348.9**	**627.1**	**+79.7%**

FIG 2. *Volume of Corporate Data Egressed by Egress Path*
Source: *The DG Data Trends Report by Digital Guardian*

When you drill into the numbers you can see just how much data egress to cloud storage services and USBs increased after COVID-19 was labeled a pandemic. In January and February 2020, we detected an average of **195 TB** per month being uploaded to cloud storage services. That number jumped to **336 TB** in March and April, a **72%** increase compared to the previous two months.

The numbers are more alarming when you compare the volume of data copied to USB devices. In January and February, we detected an average of **99 TB** per month: the volume more than doubled in the months of March and April to **221 TB.**

Uploads to cloud storage and USB devices add up to **557 TB**, or **89%** of the total **627 TB** egressed in March and April.

Digital Guardian's managed service customers have policies in place to monitor and control the movement of classified files. While blocking the action, particularly during the COVID-19 pandemic, when so many employees are working remotely, is not the most popular enforcement action, Digital Guardian's managed service analysts are monitoring and logging data movement events so future investigations can occur if any event is deemed suspicious.

123% Increase

In the volume of corporate data stored to USB devices after COVID-19 pandemic declaration and the move to work from home:

- #2 path for corporate data egressed
- #1 path for classified data egressed

Volume of Classified Data Egressed After COVID-19 Pandemic Declaration

	Data Egressed (TB)	Classified (% of data)	Unclassified (% of data)
Printer	2.7	7% (0.2 TB)	93% (2.5 TB)
NAS	57	22% (12.5 TB)	78% (44.5 TB)
Cloud Storage Services	336	42% (141.1 TB)	58% (194.9 TB)
Email	10.4	57% (5.9 TB)	43% (4.5 TB)
USB Drives	221	74% (163.5 TB)	26% (57.5 TB)
	Data Egressed	**323.3**	**303.8**
	Percentage of Data Egressed	**52%**	**48%**

FIG 3. *Volume of Corporate Data Egressed by Egress Path*
Source: *The DG Data Trends Report by Digital Guardian*

Following the WHO's pandemic declaration in March and move to work from home, **more than half** of the data moved outside of companies was classified data. Nearly three quarters of data egressed via USB in March was also classified. The majority of data egressed via email was classified too. The amount of classified data egressed from the combination of cloud storage and USBs represented **94%** of the total classified data moved in March.

While most of the data egressed via cloud storage services was unclassified, the sheer volume of files uploaded to services like Google Drive and Dropbox **(336 TB)** exceeded all other egress paths combined. While all would acknowledge it's very easy and convenient to upload data to a cloud storage folder, organizations need to better understand the nature of data that is moving to the cloud.

USB was responsible for **221 TB** of egressed data, suggesting there could be some ease of use at play here as well. Given shelter-at-home orders, sharing a USB with a co-worker or legitimate business partner is no longer easy. This could mean employees are storing large numbers of files as a backup for their own use.

In some cases, this could be legitimate use, but even in those cases, the volume of classified information now sitting on USB devices in employee homes poses a significant risk of future data loss.

The fact that some email services cap the size of attachments - Gmail and Yahoo limit attachments to 25 MB, Outlook generally caps attachments at 20 MB – may have deterred employees from sending large files via email. According to our data, only **10.4 TB** of data was egressed via email. It's still possible that more motivated employees used email to move classified files (such as trade secrets or design documents) just in reduced file size formats (i.e. images or PDF files).

These data points all point to the importance of controls that protect data at the endpoint.

Endpoint Data Loss Prevention (DLP), with its ability to see and stop risky behavior when users are off the corporate network is a proven option for security teams. DLP as a managed service goes one step further by adding the dedicated security expertise needed to provide 24x7 monitoring of sensitive data.

See: DLP as a Managed Service

A Primer on Data Security Enforcement Actions

Data Loss Prevention (DLP) solutions offer various data security enforcement actions which vary by channel and platform. The most basic enforcement option is 'Block' whereby the activity is stopped when a policy violation is detected. An email might be filtered, a file not transferred to a USB drive, or a URL made inaccessible. Most products also include other options, such as:

Encrypt

Encrypt the file or email before allowing it to be sent or stored.

Quarantine

Move the email or file into a quarantine queue for review and approval.

Shadow

Allow a file to be moved to USB storage, but send a protected copy to a central server for later analysis.

Justify

Warn the user that this action may violate policy and require them to enter a business justification to store with the incident alert on a central server.

Change Rights

Add or modify the file's digital rights management.

Change Permissions

Modify file permissions.

External Adversaries Taking Advantage of COVID-19 Uncertainty

Since March 11, advanced threats and malicious activity are up across the board, suggesting a connection to COVID-19 contributed to the spike. Cybercriminals profiteering during a global crisis isn't new, so while these findings are not surprising, security teams must be placed at a heightened state of alert.

Significant Increase in Advanced Threat Activity After COVID-19

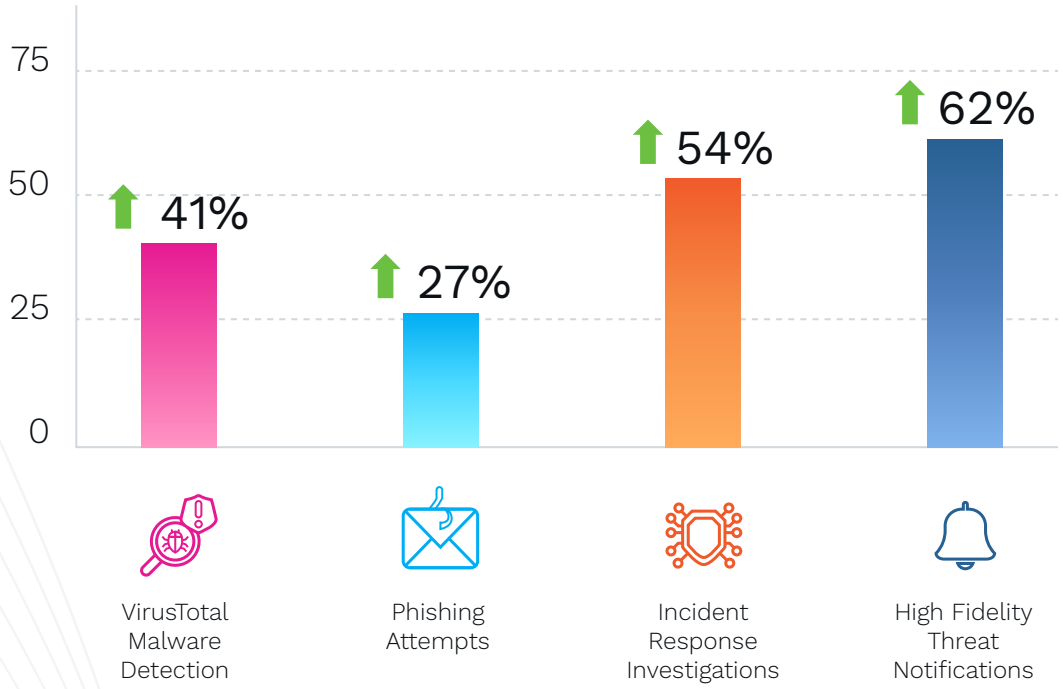


FIG 4. *Increase in Advanced Threat Activity After COVID-19*
Source: *The DG Data Trends Report by Digital Guardian*

For Digital Guardian's Managed Detection & Response customers, this sharp increase in malicious activity has coincided with an increase in high fidelity threat notifications **(62%)**, essentially any activity that results in a verified, actionable alert from a Digital Guardian Threat Analyst. Those have in turn led to an increase in incident response investigations, **54%** more than prior to the WHO's pandemic declaration.

The data also indicates a **41%** jump in endpoint infections that can be attributed to known signatures, metadata, and signals from the malware scanning service VirusTotal, indicating some bad actors, likely motivated by the shift to working from home, are using old tricks and assuming remote workers are more vulnerable. Our data also validates an uptick in phishing attempts that many security vendors have been reporting.

Judging from our data, the FBI's warnings[1] about Coronavirus phishing scams, business email compromises, and malware are well-warranted.

For example, the use of Coronavirus-themed phishing emails (see Fig. 5) is now very common. These hastily written messages frequently contain atrocious grammar, misspelled subject lines or words, and sloppy punctuation - tell-tale signs an email may not be what it seems.

More advanced attacks come from spoofed sender addresses, a trick used by phishers to evade detection. A routine analysis of the email's payload reveals the document, attached, is indeed malicious and is even named **"covid-19.exe" (see Fig. 5).**

[1] See: https://www.fbi.gov/coronavirus

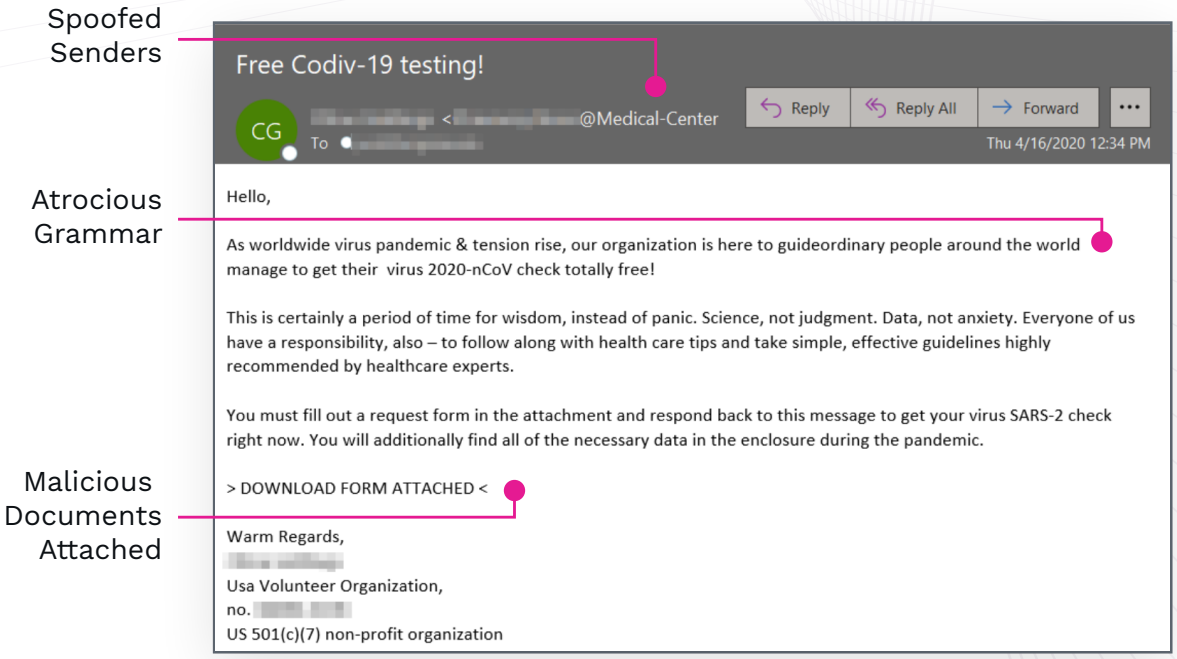


FIG 5. *Sample COVID-19 phishing email.*
Source: *@MsftSecIntel*

Without inbound filtering and defenses to prevent phishing, these emails, which appear legitimate by hiding the sender's identity, can slip through and trick users if they're not paying attention.

Digital Guardian has observed more damaging threats as well, like Coronavirus-themed malware that overwrites the Master Boot Record (MBR) of the victim's hard disk and sites pretending to offer free Netflix subscriptions when they're actually harvesting credentials.

There's been an uptick in threats targeting the healthcare sector specifically, including hoax sites masquerading as legitimate health sites that are laden with links to malware and an influx of ransomware activity targeting the healthcare industry. Detecting and stopping these types of externally based threats requires both technology and teams that can interpret patterns associated with advanced threats.

Endpoint detection and response provides part of the solution, but the experts who can respond to these advanced alerts are just as important. Spinning up a Security Operations Center (SOC) takes time and many organizations struggle to find and retain security analysts and threat hunters in the tight security market. This explains the increasing popularity of Managed Detection and Response (MDR) services.

Companies are now outsourcing advanced detection & response more than ever. With the security landscape growing more complex, and the costs of maintaining adequate in-house security teams high, it makes sense to outsource the tasks of threat hunting and response to ensure that they can promptly identify potential threats and react swiftly to mitigate damages. Because Managed Detection and Response providers play an integral role in maintaining a company's security posture, it's vitally important to carefully weigh all considerations when selecting an MDR provider. To help you understand the various factors and other considerations you should evaluate when selecting a provider, Digital Guardian reached out to a panel of data security experts and asked them to answer this question:

"WHAT ARE THE TOP CONSIDERATIONS FOR CHOOSING A MANAGED DETECTION AND RESPONSE PROVIDER?"
You can read their responses here

Five Tips to Protect Data in the Age of COVID-19

Now more than ever, it's crucial for those in charge of protecting data to remain vigilant. Security teams need to be aware of the extraordinary opportunity COVID-19 has granted to employees and external adversaries. The increasing risk to data must be considered and mitigated. Given the current economic landscape, having the majority of business professionals working remotely – many with access to the company's sensitive data, on systems not originally configured to handle this situation – amounts to an unprecedented threat to business information.

To better equip themselves, security leaders and their teams should consider the following recommendations:

1 **Issue Data Governance Policy Reminders**
Whether it's via email, Slack, Microsoft Teams or another method, now is a good time to remind employees of the company's policies for handling business and customer data. Reiterate to employees the importance of using only company-sanctioned apps, cloud storage and USB drives when it comes to moving and storing sensitive information.

2 **Label Sensitive Information**
Ensure any and all highly sensitive data is classified as such. Label sensitive information like intellectual property, financial information, healthcare, and information subject to compliance regulations. Double check that policies are in place to prevent unauthorized access. These labels can be human readable or machine readable. Even using a simple digital watermark can act as a subtle reminder to users that they are accessing protected information. That knowledge alone can be enough to reduce the risk of unwanted activity.

3 **Limit Access to Sensitive Data**
Even without a formal data loss prevention program or technology solution in place, you can reduce the risk of data loss. Simply inventory the users that have access to sensitive file shares and other data repositories, assess their need for that access and limit it for those that don't require access.

4 **Host a Remote Security Awareness Training Session**
Many organizations have grown accustomed to hosting the annual or bi-annual in-classroom security awareness training session. With the onset of COVID-19 however, these in-classroom experiences can no longer occur. There are numerous companies that can offer remote and/or on-demand security awareness trainings that should be considered.

5 **Consider Deploying Virtual Desktop Infrastructure (VDI) or Desktop as a Service (DaaS)**
With the March 11 declaration of COVID-19 as a pandemic and the follow-up stay-at-home orders, many "work from office" organizations were forced to transform to "work from home" overnight. For some companies, this has meant employees working from their personal PCs or laptops, leveraging their home Wi-Fi networks. This is a high-risk situation and organizations have a limited ability to enforce security controls in these circumstances. It appears COVID-19 will be with us for many months to come, so organizations should consider moving employees off personal devices to corporately managed virtual endpoints hosted in the cloud. VDI and Desktop-as-a-Service (DaaS) providers such as Amazon Workspaces can reduce the risk by providing strong controls on remote workstations while still allowing the system and data access employees need to do their job.

Additional Resources

Readers of this report may also find these additional resources useful:

- The Definitive Guide to DLP (2020 Edition)
- SC Media Labs DLP Comparison Report
- Gartner Report: How to Overcome Pitfalls in Data Classification Initiatives
- Digital Guardian Technical Overview

Report Methodology

For this report, Digital Guardian aggregated and anonymized data from 194 customers in our Managed Service program. These companies represent a broad swath of industries and firm sizes across the globe. The data set analyzed was from January 1 – April 15, 2020 and comparative data was evaluated from January 1 – February 29, 2020 (before the global onset on COVID-19) vs. March 1 – April 15, 2020 (after the COVID-19 pandemic came to the forefront).

This subset of Digital Guardian customers comes from some of the most data-intensive industries and they rely on both regulated and structured data as well as unstructured intellectual property for competitive advantage. Since March 1, 2020 when the WHO began monitoring and reporting on COVID-19 globally, the Digital Guardian team noticed a marked change in customer data usage patterns. Digital Guardian, via our endpoint agent, collected over 45 billion data events, all pointing to a dramatic shift in behavior from the COVID-induced changes in business operations.

A detailed breakdown of the organizations included in the data set is highlighted below.

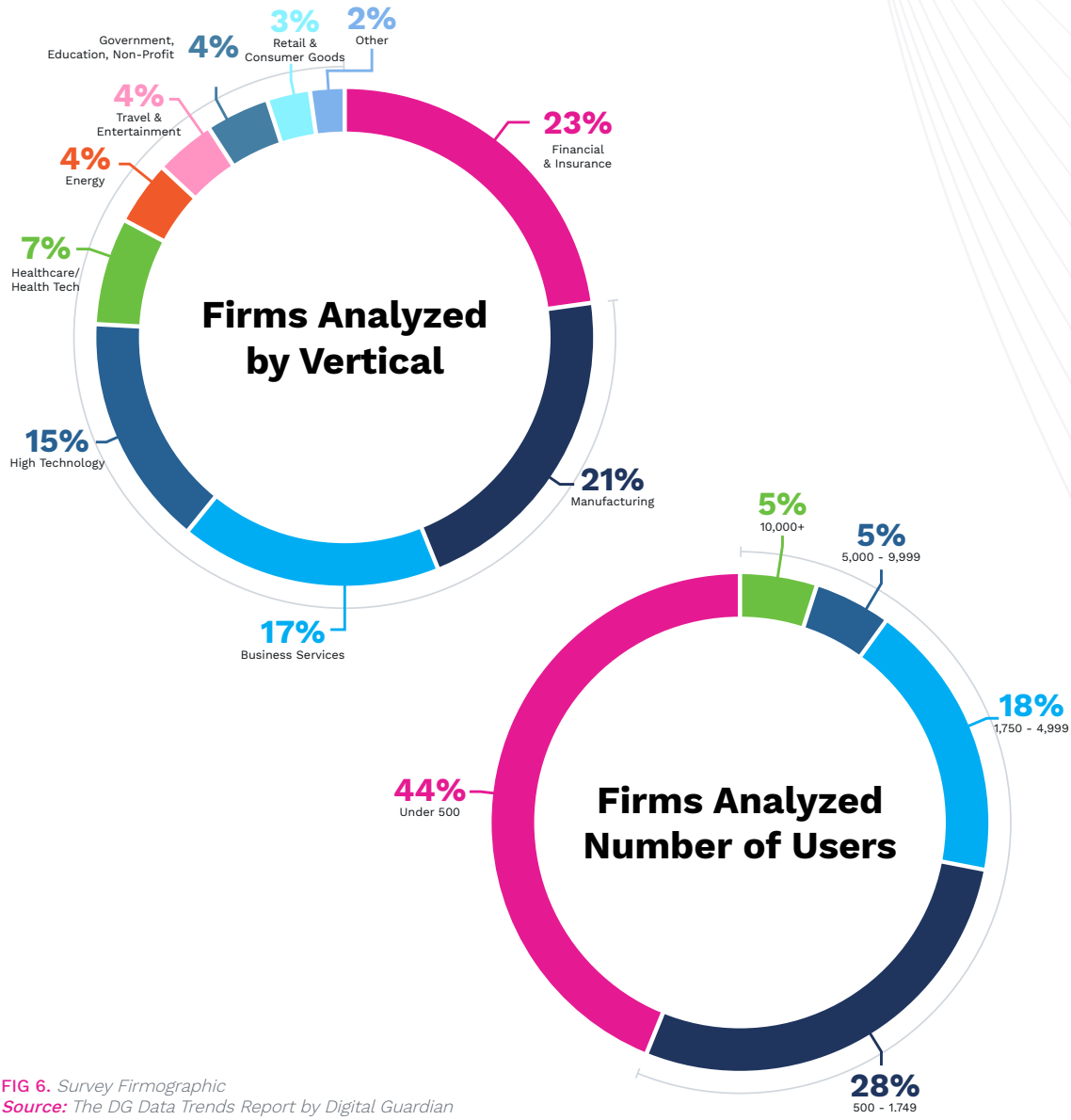


FIG 6. *Survey Firmographic*
Source: *The DG Data Trends Report by Digital Guardian*

About Digital Guardian

Digital Guardian is no-compromise data protection. The company's cloud-delivered data protection platform is purpose-built to stop data loss by both insiders and outsiders on Windows, macOS, and Linux operating systems. The Digital Guardian Data Protection Platform performs across the corporate network, traditional endpoints, and cloud applications. For more than 15 years, we have enabled data-rich organizations to protect their most valuable assets with a choice of SaaS or fully managed deployment. Digital Guardian's unique policy-less data visibility and flexible controls enable organizations to protect data without slowing the pace of their business. To learn more please visit: https://digitalguardian.com/

Digital Guardian Managed Services Program

Digital Guardian's Managed Security Program (MSP) acts as a remote extension of your security team and offers data protection as a managed service. Our security experts will host, administer, and run your data security platform leveraging the Digital Guardian Data Protection Platform which is powered by AWS. Our 24x7 global analyst teams have deep experience and expertise in data protection and will help you contain insider and outsider threats before sensitive data leaks out of your organization.

DIGITAL GUARDIAN®

CORPORATE HEADQUARTERS
275 Wyman St., Suite 250
Waltham, MA 02451 USA
info@digitalguardian.com
781-788-8180
www.digitalguardian.com

SHARE