

The logo features a large, light blue circle with a thick, dark blue ring inside it. A horizontal line passes through the center of the circles. To the right of the main circle, a thin white arc with two small blue circles at its ends extends towards the right edge of the frame.

PROLINK

Canada's Insurance Connection

THE CLOUD: NOT JUST A PLACE TO DAYDREAM ANYMORE

2020

How can SMBs balance the benefits of using the cloud and cloud-based services, while managing the associated risks?

TABLE OF CONTENTS

Introduction	01
Overview of Cloud and Cloud Service Models	02
Benefits of Cloud Computing	04
Drawbacks of Cloud Computing	05
Consequences of a Data Breach in the Cloud	08
Cloud Risk Management Strategies for SMBs	10
The Future Is Cloud	12
Works Cited	14



INTRODUCTION

Historically, data processing and storage has occurred on-premises, proprietary servers, requiring hefty financial investments in hardware, software, and upkeep. If a company ever wanted to increase its storage, it would have to purchase more physical space. But with rapid digitalization, the growing demands of modern businesses require computing technology that traditional data centres can no longer meet.

Enter the cloud. The term “cloud” these days most often refers to a complex infrastructure used to store, manipulate, and process data.

Cloud services are delivered online by organizations known as “**Cloud Services Providers**” (CSPs), which charge a monthly fee to manage data. With the cloud, increasing your storage or processing power is as simple as increasing your monthly subscription. The cloud is flexible, accessible, and affordable—so it’s no wonder that **90% of companies use some form of cloud services in their operations.**¹

While iterations of the cloud have been around for many years, it’s only recently that businesses have fully begun to embrace its computing potential. **But, is there a price to constant connectivity? And do all users fully understand their responsibilities when it comes to protecting data in the cloud?**

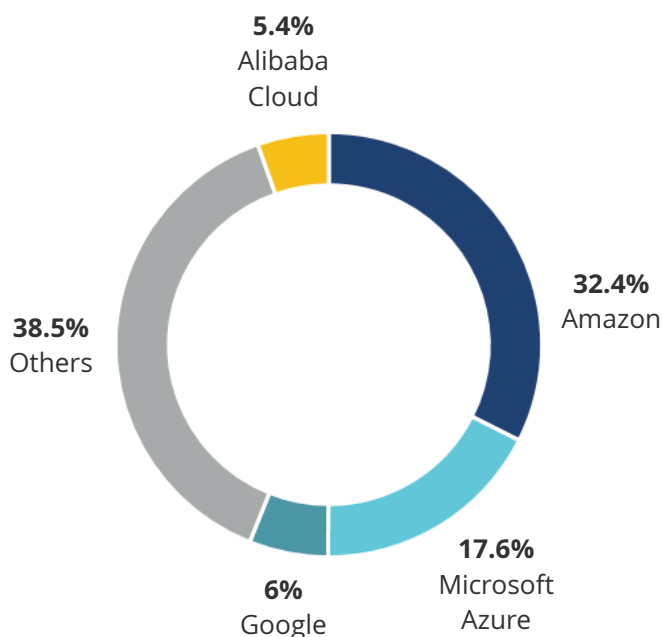


FIGURE 1. The key CSPs by market share as of Q4 2019. Amazon Web Services (AWS) dominates the market.²

IN THIS WHITE PAPER, DISCOVER THE:

1. Different cloud service delivery models;
2. Upside of cloud computing;
3. Downside associated with the cloud;
4. Measures SMBs can take to balance the benefits and risks of the cloud;
5. The future of the cloud for SMBs.

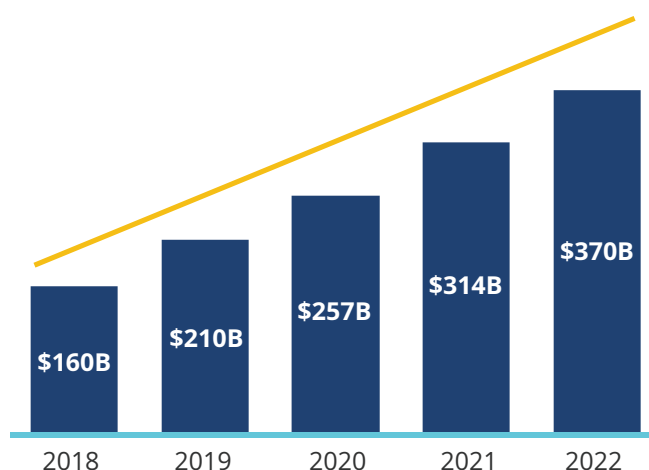


FIGURE 2. Projected worldwide spend on cloud computing. With a Compound Annual Growth Rate (CAGR) of 23%³, the cloud isn’t going anywhere.

1. “Cloud Computing Trends: 2019 State of the Cloud Survey”, Flexera, February 27, 2019, <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/>.

2. “Cloud market share Q4 2019 and full-year 2019,” Canalys, February 4, 2020, https://www.canalys.com/static/press_release/2020/Canalys---Cloud-market-share-Q4-2019-and-full-year-2019.pdf.

3. “Worldwide Public Cloud Services Spending Forecast to Reach \$210 Billion This Year, According to IDC”, IDC, February 28, 2019, <https://www.idc.com/getdoc.jsp?containerId=prUS44891519>.

DO YOU KNOW WHAT KIND OF CLOUD YOU'RE USING?

There are many different cloud service delivery models available, and each require a different level of system administration, ranging from highly involved to none-at-all.⁴ The different cloud service models can be used on their own, or in tandem to fulfill various business needs. Read about the different kinds of cloud structures your business could be using below.

MOST LIKELY, YOUR COMPANY USES:

Cloud computing services fall into three categories, known as the “**Cloud Computing Stack**”, because they often build on top of one another:

Infrastructure-As-A-Service (IaaS): Storage, networking, and virtualization services, geared at replacing the proprietary, physical servers of the past. With IaaS, companies can dynamically modify their infrastructure based on their storage needs, eliminating the hard costs associated with maintaining on-premises servers. Examples include Amazon Web Services (AWS) and Microsoft Azure.

Platform-As-A-Service (PaaS): Services that allow developers to quickly create applications without having to focus on software or security updates. Essentially, developers can “decorate” the virtual space within the tool to fit their needs, without worrying about the external structure that houses the space itself. PaaS is usually built on top of IaaS, like the Google App Engine.

Software-As-A-Service (SaaS): Out-of-the-box services accessed by logging into an online application through any device with an internet connection. Users simply need a User ID and password. SaaS platforms are built on top of IaaS or PaaS. Examples include Google Apps, Adobe, Dropbox, and more.

ANOTHER LAYER OF COMPLEXITY:

The environment that your cloud “lives” in can vary too. There are three types of cloud⁵:

Public Cloud: Services may be free, subscription-based, or usage-based. The environment (hardware, software, and other infrastructure) is managed by the Cloud Services Provider (CSP), and multiple organizations (also called tenants) can access the same resources online. Email, development environments, and online Microsoft Office applications are all examples of public cloud.

Private Cloud: Services are limited to a single tenant and can be hosted on or off-premises. This model is more expensive and requires more internal resources to maintain. As a result, mostly financial institutions, governments, and larger businesses tend to use this type of cloud.

Hybrid Cloud: The combination of private and public clouds. Typically, high-volume and low-security operations run in the public cloud, and sensitive operations run in the private cloud. It can also refer to a cloud service combined with on-premises infrastructure.

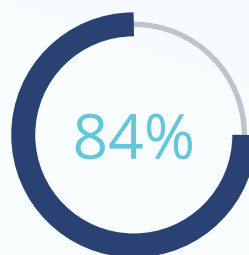


FIGURE 3. 84% of enterprises employ a **MULTICLOUD** strategy (a subset of hybrid cloud) with multiple public and private clouds from multiple vendors.⁶

4. Tony Hou, “IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More”, *Big Commerce* (blog), Accessed March 9, 2020, <https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-key-differences-between-on-premise-saas-paas-iaas>.

5. “What Is a Public Cloud? | Public Cloud vs. Private Cloud”, *Cloudflare*, Accessed March 6, 2020, <https://www.cloudflare.com/learning/cloud/what-is-a-public-cloud/#:>

6. Laurence Goasduff, “Why Organizations Choose a Multicloud Strategy”, *Gartner*, May 7, 2010, <https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy>.

HOW DO SMBs USE CLOUD COMPARED TO ENTERPRISES?

84% of enterprises employ a multicloud strategy.⁷ Why? Using multiple private and public clouds from various providers enables better disaster recovery in the event of an outage and prevents vendor lock-in—the over-reliance on one particular vendor—and ultimately allows different companies to respond to the different needs of a business.⁸

What about SMBs? Are they using public, private, or hybrid clouds? Studies show that SMBs use public cloud services more than private ones.⁹ With public cloud spend growing three times faster than private cloud spend, it seems that the (often cheaper) public cloud is winning the race.¹⁰

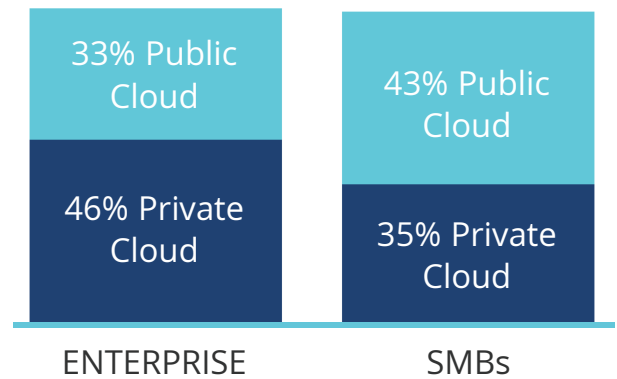


FIGURE 4. SMBs prefer to use public cloud over private cloud while the opposite holds true for enterprises.¹¹

HOW DO DIFFERENT INDUSTRIES USE CLOUD?

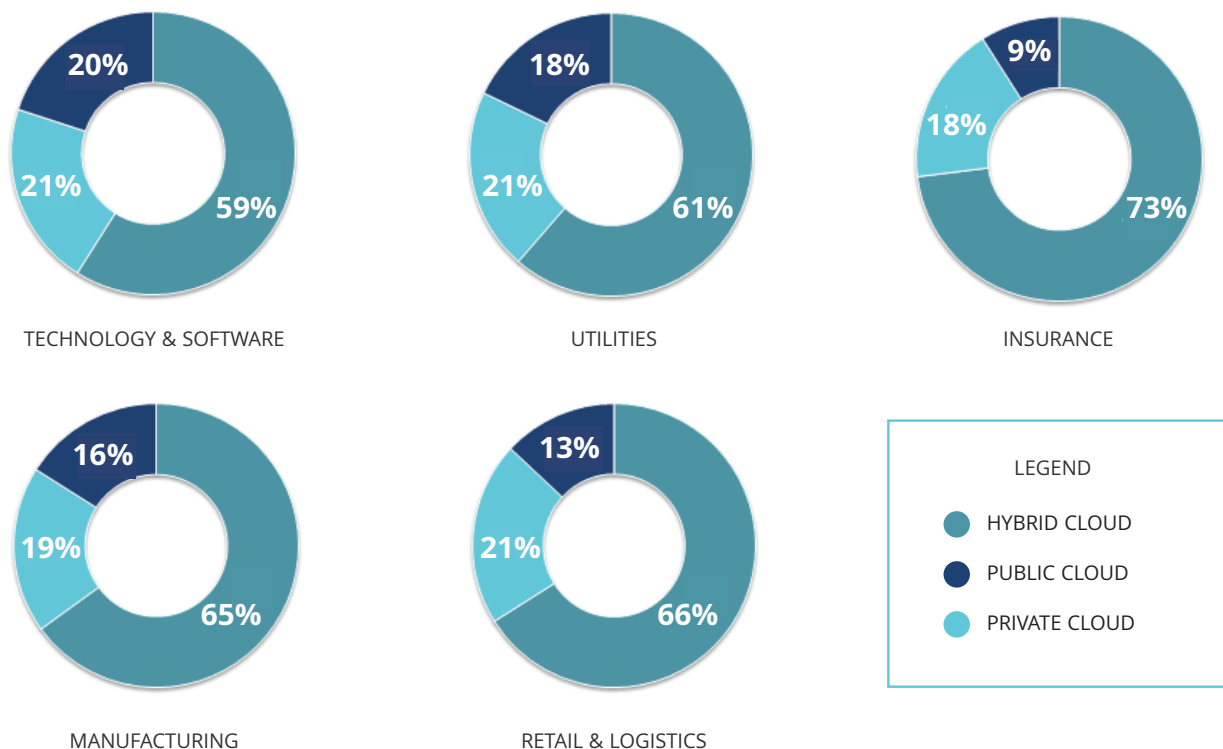


FIGURE 5. While the most prevalent cloud type varies by trade, hybrid cloud appears to be the leading strategy when looking across all industries.¹²

7. Laurence Goasduff, "Why Organizations Choose a Multicloud Strategy", *Gartner*, May 7, 2010, <https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy>

8. Laurence Goasduff, "Why Organizations Choose a Multicloud Strategy", *Gartner*, May 7, 2010, <https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy>

9. "Cloud Computing Trends: 2019 State of the Cloud Survey", *Flexera*, February 27, 2019, <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/>

10. "Cloud Computing Trends: 2019 State of the Cloud Survey", *Flexera*, February 27, 2019, <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/>

11. "Cloud Computing Trends: 2019 State of the Cloud Survey", *Flexera*, February 27, 2019, <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/>

12. Ani Miteva, "8 cloud adoption statistics that reveal the future of the cloud", *Cloud Worldwide Services*, March 20, 2018, <https://www.cloudworldwideservices.com/en/cloud-adoption-statistics-cloud-future/>

WHAT ARE THE BENEFITS OF CLOUD COMPUTING?

OVER 70% OF CFOs SAID CLOUD COMPUTING HAD A HUGE IMPACT ON THEIR BUSINESS AND THEIR BOTOM LINE.¹³

How? The key advantages of cloud computing for businesses are summarized below:

01

COST SAVINGS

Since most cloud systems operate on a metered, pay-as-you-go basis, businesses are only charged for as much space and processing power as they need to serve stakeholders and clients day-to-day. 82% of SMBs reported cost savings as a result of cloud, and 70% reinvested their savings into their business.¹⁴

02

FLEXIBILITY

Rather than undergoing complex IT upgrades for additional storage or processing power, CSPs can provide the customization a business needs by instantly adding extra capacity for a nominal usage fee or removing said capacity when peak periods subside to save money.

03

COLLABORATION

When data is centrally maintained, physical distance does not impede efficiency. Companies can cater to dynamic work arrangements by allowing workers to collaborate and connect on-the-go through cloud-based workflow.

04

SCALABILITY

By removing the work that comes with IT hosting and infrastructure, companies can redirect their time, attention, and resources towards developing and deploying new products, applications, and services at scale.

The cloud probably sounds pretty great right now—and don't get us wrong, it is.

But before you move all of your mission-critical functions onto the cloud, you need to understand the risks of cloud computing and the steps you can take to reduce them. With appropriate risk management strategies in place, your business can take full advantage of the cloud.

13. Victoria Wilson, "10 Cloud Computing Statistics You Need To Know", Sys Group, Accessed March 3, 2020, <https://www.sysgroup.com/resources/blog/10-cloud-computing-statistics-2018>.

14." Driving growth together: Small businesses and the cloud", Office 365, Accessed March 14, 2020, <https://info.microsoft.com/rs/microsoftdemandcenter/images/driving-growth-together-small-businesses-and-cloud-infographic.pdf>.

WHAT ARE THE DRAWBACKS OF CLOUD COMPUTING?

The nature of cloud computing requires companies to cede control of their most valuable asset: data. Whether it's client information, employee files, trade secrets, or even financial reports, putting any data in the cloud makes privacy law compliance, security, data leakage, and even business continuation a top concern for most IT professionals.

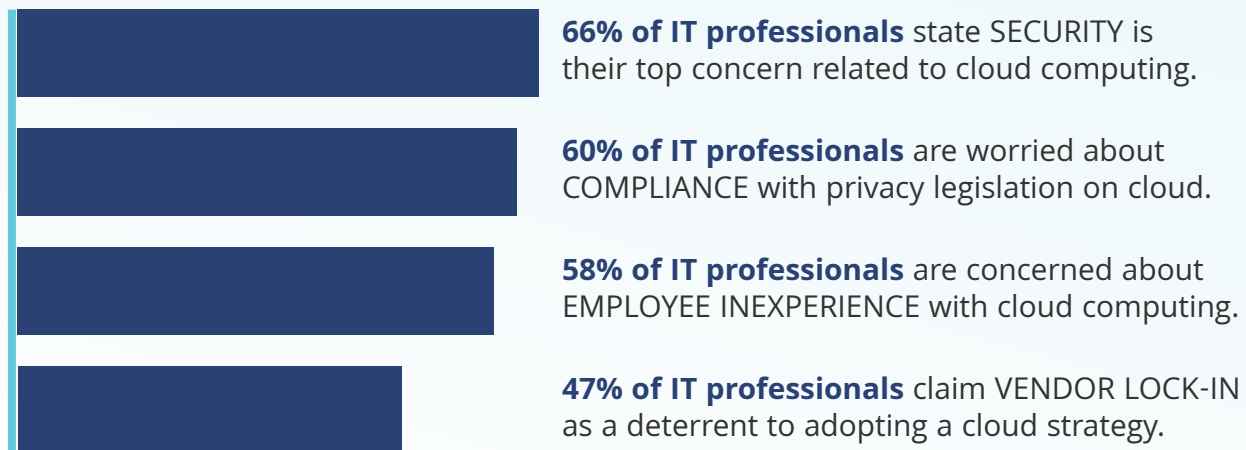


FIGURE 6. The top concerns cited by IT professionals when implementing cloud strategies.¹⁵

These concerns can be grouped under three main categories: **SECURITY, RELIABILITY, and LIABILITY.**

RISK 1. SECURITY

While the network and infrastructure of the cloud is controlled by a CSP, configuration of the cloud (setting it up to serve your specific needs) always falls on the user. Although CSPs are not immune to hacking, **the truth is that 95% of cloud security failures are the user's fault.**¹⁶ How?

MISCONFIGURATION RISK

Mismanaged permissions controls, lack of audit or governing controls, lack of logging, firewall misconfiguration, or even ignoring CSP-suggested controls, all contribute to **"misconfiguration of the cloud,"** an umbrella term used to describe a situation where computing assets are not set up properly, leaving data exposed to malicious activity.¹⁷ Experts say misconfiguration errors can be caused by subcontracting work to external vendors, missing something in the instruction manual (often over 140 pages), or even simple laziness.¹⁸

The consequences of misconfiguration depend on your cloud service delivery model. SaaS, for example, is relatively low-risk compared to IaaS. A 2019 study performed by McAfee shows that 99% of misconfigurations in IaaS environments go undetected, and **despite the fact that enterprises report only 37 misconfiguration incidents per month, data places the real number at 3,500 per month.**¹⁹

15. Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020", *Forbes*, January 7, 2018, <https://www.forbes.com/sites/louiscolumnbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#76eeabe46261>.

16. Kasey Panetta, "Is the Cloud Secure?", *Gartner*, October 10, 2019, <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>
17. Dennis Leber, "Behind The Data Breach: Understanding Cloud Security And Misconfigurations", *Cyber Security Hub*, September 17, 2019, <https://www.cshub.com/cloud/articles/behind-the-data-breach-understanding-cloud-security-and-misconfigurations#>.

18. James Rundle, "Human Error Often the Culprit in Cloud Data Breaches", *Wall Street Journal*, August 27, 2019, <https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203>.

19. "Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report", *McAfee*, 2019, <https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/rp-cloud-adoption-risk-report-iaas.pdf>.

EMPLOYEE RISK

Chances are: your staff has varying degrees of digital competency. And yet, the cloud allows everyone (more-or-less) equal access to your data. If an employee falls prey to a phishing scam, an outsider could breach your accounts. Alternatively, if an employee is using similar passwords across multiple websites and applications, their credentials could easily be stolen and used to compromise your company's information.

PARTNER RISK

One of the great selling points of cloud computing is how easy it is to connect your data and operations with partners all over the world. But you don't always know exactly how your partners are using your data. Or if they've misconfigured their own servers. In many cases, your partner can become a gateway to your information. And unfortunately, even the biggest companies have been exposed by this risk, like Facebook as recently as April 2, 2019.²⁰ Accurate visibility of data flow in the cloud remains a challenge for most businesses.

A WORRYING DISCONNECT

93% of organizations are moderately-to-extremely concerned about cloud security, and 66% of IT professionals claim that traditional security solutions don't work in the cloud.²¹ Nonetheless, 84% of organizations are moderately-to-extremely confident in their ability to manage cloud risk.²² While it's true that CSPs can offer more robust safety measures than the average SMB, business owners should not be lulled into a false sense of security. CSPs are not infallible, and even if they are, much of the risk stems from the SMB itself.



FIGURE 7. Organizational attitudes on cloud security.²³

As companies migrate their workloads online, cloud platforms continue to amass large volumes of high-value data at an exponential rate and, in turn, invite increasingly sophisticated forms of cybercrime. Privacy breaches that expose consumer data can lead to the identity theft of affected individuals, diminish client trust, and leave companies liable for compliance violations with new global privacy laws.

20. Chris Pedigo, "The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020", *Lacework* (blog), December 13, 2019, <https://www.lacework.com/top-cloud-breaches-2019/>.

21. "Cloud Security Report", *Cybersecurity Insiders*, 2019, <https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/>.

22. "Cloud Security Report", *Cybersecurity Insiders*, 2019, <https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/>.

23. "Cloud Security Report", *Cybersecurity Insiders*, 2019, <https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/>.

RISK 2. RELIABILITY

When data is housed over a remote server, continuous, responsive service is not always possible. This is partly due to the growing threat of Distributed Denial of Service (DDoS) attacks in which hackers send unprecedented volumes of traffic to cloud-based applications with the intention of crashing the servers.²⁴ CSPs attempt to address this concern with redundancy techniques that store the same information on multiple servers with different power supplies.²⁵ Even so, their systems could still fail and leave clients with no way to process payments or reach saved files. Without direct access to cloud networks, businesses must rely on the prompt action of the cloud provider if there is ever a service interruption.

The risks associated with the availability of cloud platforms are less severe than cybercrime, but can still be damaging to a business’s operations, income, and reputation. Depending on the cloud’s importance to a company’s day-to-day operations, an outage can be anything from a minor inconvenience to a massive and costly disruption. In 2019, 34% of businesses that suffered a cloud outage experienced losses resulting over \$1 million.²⁶

RISK 3. LIABILITY

Misconceptions about accountability for cloud storage keeps many organizations from taking reasonable steps to protect their data. Often, companies wrongly assume that the transfer of data offsite entails with it the implicit the transfer of security risk. However, cloud systems operate on a model of shared responsibility wherein both the CSP and the user are responsible for different components of security. In fact, under every cloud service model available, the onus for user access and data always falls on the business itself. **Shockingly, only 32% of companies believe that protecting data in the cloud is their responsibility.**²⁷

Experts predict that by 2025, 99% of security failures will be the user’s fault, and 90% of businesses that cannot adequately control cloud security will mistakenly share sensitive data.²⁸ As countries tighten their data protection legislation, businesses may be held liable for massive damages in the event of a breach.

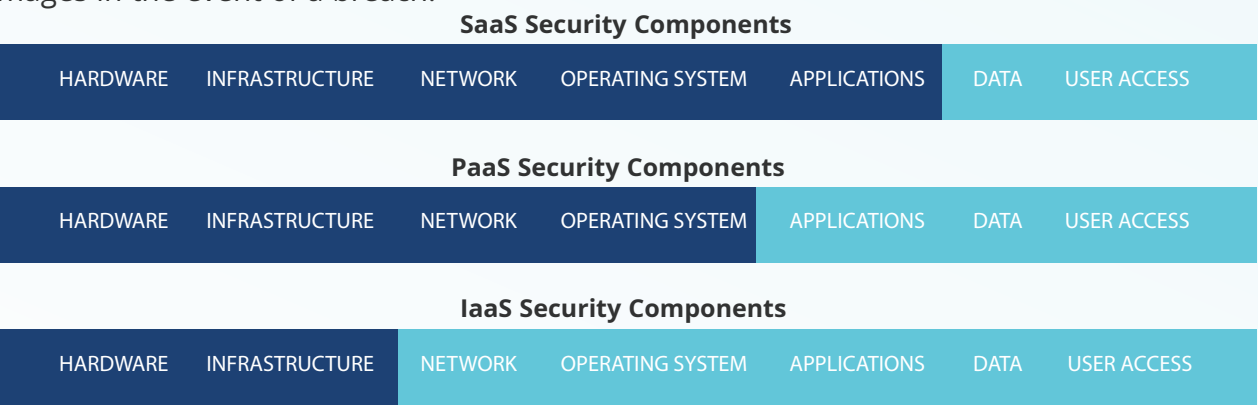


FIGURE 8. The chain of responsibility for cloud security.²⁹ In all models, data is the responsibility of the business owner.

24. Gilad Mayaan (GiladMayaan), “Top Cloud Data Security Challenges and How to Overcome Them”, *IBM Developer*, September 20, 2019, <https://developer.ibm.com/recipes/tutorials/top-cloud-data-security-challenges-and-how-to-overcome-them/>.
25. Gilad Mayaan (GiladMayaan), “Top Cloud Data Security Challenges and How to Overcome Them”, *IBM Developer*, September 20, 2019, <https://developer.ibm.com/recipes/tutorials/top-cloud-data-security-challenges-and-how-to-overcome-them/>.
26. Timothy Zeilman, “Is your data in the cloud? It’s still at risk of cyberattack”, *NU Property Casualty 360*, February 28, 2019, <https://www.propertycasualty360.com/2019/02/28/is-your-data-in-the-cloud-its-still-at-risk-of-cyberattack/?slreturn=20200214214758>.
27. “48% of corporate data is now stored on the cloud”, Panda, October 17, 2019, <https://www.pandasecurity.com/mediacenter/security/cloud-security-encryption/#:>
28. Kasey Panetta, “Is the Cloud Secure?”, *Gartner*, October 10, 2019, <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>
29. Eric Dosal, “7 Cloud Security Challenges and Risks to Be Aware Of”, *Compuquip Cyber Security* (blog), March 5, 2020, <https://www.compuquip.com/blog/cloud-security-challenges-and-risks>.

WHAT ARE THE CONSEQUENCES OF A DATA BREACH?

OVER TWO THIRDS OF BUSINESSES HAVE FAILED TO APPLY PROCEDURES IN LINE WITH DATA PROTECTION LAWS.³⁰

To combat the growing threat of cybercrime, government and industry bodies across the world have introduced extensive privacy laws for all organizations that store personal data. These mandates, like the European Union's General Data Protection Regulation (GDPR) and **the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)**, are intended to strengthen accountability for unsecured data and penalize companies for the failure to safeguard, retain, or dispose of any personal information in their custody.

Despite these efforts, trends from the past three years show that businesses are continuing to use cloud applications and platforms without proper security defenses. Recent reports show that **only 54% of companies know where their sensitive data is stored at all.**³¹ Evidently, organizations are struggling to balance the integration of cloud services with regulatory compliance, leaving themselves exposed to dire legal, financial, and reputational consequences.

1. LEGAL REPERCUSSIONS

Data is subject to the rules and requirements of the region in which it is processed and where the client resides. Companies must know where their data resides, who has access to it, and how it is protected. And in the event of a breach, they must alert all victims and appropriate governing bodies. Since cloud storage typically entails the cross-border transfer of information, companies must be sure to abide by any and all privacy laws specific to the physical location of their chosen service provider. The GDPR, for example, is applicable to the personal data of all EU residents, regardless of where the information is stored and who is storing, processing, or using it.

Regardless, while 71% of Canadian businesses reported experiencing at least one cyberattack in 2019, an alarming 43% were still unaware of PIPEDA's mandatory breach disclosures.³² Unless companies take reasonable steps to secure client data, they risk severe penalties for any compliance violations. If an organization is found negligent of an offence under PIPEDA (or any applicable provincial legislation), they could be held **liable for up to \$100,000 in fines.**

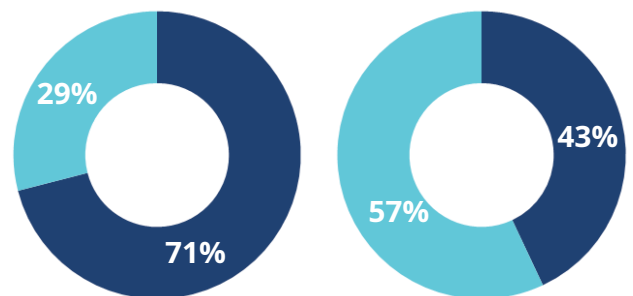


FIGURE 9. 71% of Canadian businesses experienced at least one breach in 2019, and surprisingly, 43% of organizations were not aware of their obligation to disclose a breach to the Privacy Commissioner.³³

30. "Businesses collect more data than they can handle, reveals Gemalto", *Gemalto*, July 10, 2018, <https://www.gemalto.com/press/pages/businesses-collect-more-data-than-they-can-handle-reveals-gemalto.aspx>.

31. "Businesses collect more data than they can handle, reveals Gemalto", *Gemalto*, July 10, 2018, <https://www.gemalto.com/press/pages/businesses-collect-more-data-than-they-can-handle-reveals-gemalto.aspx>.

32. "2019 CIRA Cybersecurity Survey", *CIRA*, Accessed March 4, 2020, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>.

33. "2019 CIRA Cybersecurity Survey", *CIRA*, Accessed March 4, 2020, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>.

2. FINANCIAL CONSEQUENCES

When it comes to cloud computing, it is the duty of the data owner—not the CSP—to protect client information and assume financial responsibility. Data breaches are costly and can be crippling for SMBs who often have minimal budget for cybersecurity to begin with. In 2019, the average cost of investigating and remediating a breach among Canadian organizations was **\$9.25 million**.³⁴

The expenses from client notification alone can easily reach into the millions—the average cost to notify clients per stolen record in Canada is \$190.³⁵ For healthcare files, that value jumps to \$429 per record.³⁶ **Breach remediation also usually includes fees for: legal counsel and defence, IT services, data restoration, public relations assistance, credit monitoring, and disciplinary action.** Plus, there's always a possibility that victims and affected individuals may seek damages for any injury or harm caused by the breach, compounding an organization's overall losses.

Business interruption costs can make matters even worse. According to IBM, the average life cycle of a breach from discovery to containment in 2019 was 314 days.³⁷ And if a company is unable to access their records due to a breach, or their records are tied up in litigation for a significant length of time, the subsequent decline in revenue can hinder or prevent recovery altogether.

3. REPUTATIONAL DAMAGE

Depending on the severity of the breach, negative publicity can lead to a high churn rate if clients opt to take their business to a competitor. Loss of trust, diminished goodwill, and lost income as a result can do irreparable harm to the reputation of a business, especially if a company fails to take swift action, apologize to, or even inform affected individuals immediately.

According to CIRA's 2019 Canadians Deserve a Better Internet report, **only 19% of Canadians** said they would continue to do business with an organization if their personal information was compromised in a cyberattack.³⁸ **65% of Canadian businesses reported a negative reputational impact** following a breach in 2019.³⁹ Highly regulated industries such as healthcare, finance, and pharmaceuticals, are particularly vulnerable to high turnover since clients generally have higher expectations for data security.

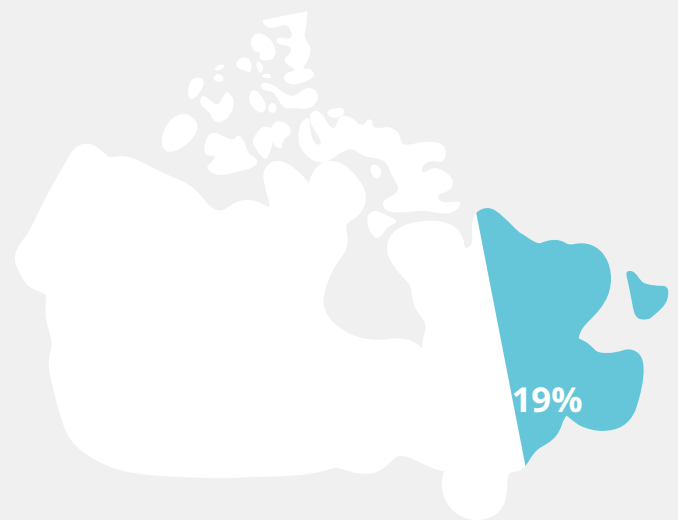


FIGURE 10. Only 19% of Canadians would continue to do business with an organization if their personal information was exposed in a cyberattack.⁴⁰

34. "2019 CIRA Cybersecurity Survey", CIRA, Accessed March 4, 2020, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>.

35. "2019 Cost of a Data Breach Report", IBM Security, Accessed March 14, 2020, <https://databreachcalculator.mybluemix.net/executive-summary>.

36. "2019 Cost of a Data Breach Report", IBM Security, Accessed March 14, 2020, <https://databreachcalculator.mybluemix.net/executive-summary>.

37. "2019 Cost of a Data Breach Report", IBM Security, Accessed March 14, 2020, <https://databreachcalculator.mybluemix.net/executive-summary>.

38. "Canadians deserve a better internet", CIRA, Accessed March 4, 2020, <https://www.cira.ca/resources/state-internet/report/canadians-deserve-a-better-internet>.

39. "CANADA | GLOBAL THREAT REPORT | DEFENDER POWER ON THE RISE", Carbon Black. Canada, October, 2019, <https://www.carbonblack.com/resources/threat-research/thank-you-45385/>.

40. "Canadians deserve a better internet", CIRA, Accessed March 4, 2020, <https://www.cira.ca/resources/state-internet/report/canadians-deserve-a-better-internet>.

HOW CAN SMBs BENEFIT FROM THE CLOUD WHILE MINIMIZING RISKS?

THE MAJORITY OF ORGANIZATIONS WILL STRUGGLE TO QUANTIFY CLOUD RISKS UNTIL 2024.⁴¹

As dependence on cloud technologies continues to grow, having a holistic strategy for sensitive data flow, protection and distribution must become a top priority for all businesses. Here are the three-major steps companies can take to protect data through every stage of the client journey:

STRATEGY 1. IMPLEMENT IN-HOUSE RISK MANAGEMENT TACTICS

1

EDUCATE EMPLOYEES: Although 96% of organizations agree that their staff would benefit from cybersecurity awareness and certification, only 41% have mandatory training in place for all team members.⁴² Keeping all staff up-to-date with cloud security best practices ensures that employees know how to spot cyber threats and what to do when they come across them.

2

APPLY ACCESS CONTROL: Limit access to resources and services to the bare minimum permissions necessary for work and block all other privileges. Proactively classifying information allows businesses to protect against the threat of malicious behaviour from rogue employees.

3

ENCRYPT DATA: Use encryption whenever and wherever possible, especially before transferring data to the cloud. If data is encrypted by a company prior to offsite storage, it can only be decrypted by authorized users. That is, data should be encrypted when it is both at-rest, and when being transmitted.

4

IMPLEMENT MULTI-FACTOR AUTHENTICATION: Multi-factor authentication, such as passwords, fingerprint ID, and dual-step security features, add extra layers of protection to business data and make it difficult for information to be hacked or stolen.

5

CREATE A BUSINESS CONTINUITY PLAN & INCIDENT RESPONSE PLAN: A Business Continuity Plan (BCP) outlines effective guidance around continued operations when a company experiences business interruption. An Incident Response Plan (IRP) is a set of processes designed to help you identify the source, method, and target of a breach, and the appropriate next steps.

41. Kasey Panetta, "Is the Cloud Secure?", *Gartner*, October 10, 2019, <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>.
42. "2019 CIRA Cybersecurity Survey", *CIRA*, Accessed March 4, 2020, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>.

STRATEGY 2. REVIEW CONTRACTS IN-DEPTH

Read up on your potential cloud service provider or business partner. Familiarize yourself with their business practices and ask the following questions:

- ✓ How long have they been in business?
- ✓ Are they up-to-date on data centre and industry certifications?
- ✓ Are they compliant with the service-specific privacy and security compliance needs of your organization?
- ✓ How experienced are they with your industry?
- ✓ Have they had a security audit in the last year? If so, will they share the results?
- ✓ Where is the data stored? Your provider may be headquartered in Canada, but they might store data in multiple centres around the world.

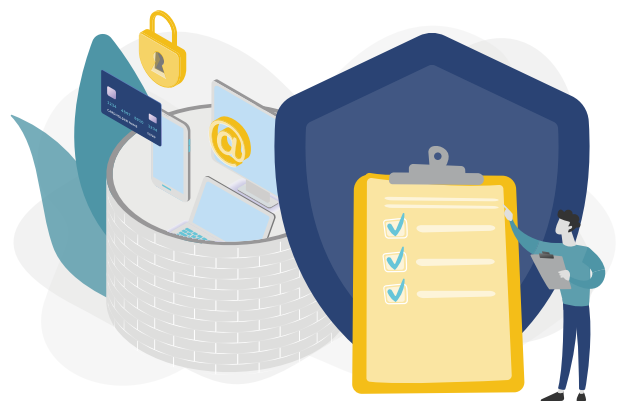
Review your contract. Data storage needs differ between industries. Before signing, make sure your contract addresses these concerns:

- ✓ How soon will you be notified if a breach is detected?
- ✓ Is the provider obligated to replace stored data if a disaster destroys their servers?
- ✓ How soon can data be restored? What kind of support will you receive if you run into any issues?
- ✓ Are there resources in place to back-up data and ensure that there cannot be any permanent loss?
- ✓ Is the process to transfer data from their servers back to your company well-defined, should the business relationship end for any reason?

STRATEGY 3. OBTAIN DATA SECURITY AND PRIVACY BREACH INSURANCE

Even if you complete your due diligence and find a cloud provider that you can entrust with your data, **you're never truly finished with cybersecurity**. Despite your best efforts, you could still experience a breach. So what else can you do? You can prepare for it with a robust Data Security and Privacy Breach Insurance policy.

Data Security and Privacy Breach Insurance is an invaluable risk management strategy for your business, particularly when you consider that 88% of Canadian businesses reported a breach in 2019.⁴³ These policies cover the specific risks associated with cyber-attacks and privacy breaches and come in many customizable options to fit your needs.



43. "CANADA | GLOBAL THREAT REPORT | DEFENDER POWER ON THE RISE", *Carbon Black. Canada*, October, 2019, <https://www.carbonblack.com/resources/threat-research/thank-you-45385/>.

DATA SECURITY AND PRIVACY BREACH INSURANCE CAN HELP YOU ACCESS:

Funds to set up credit monitoring and notification for affected parties, as well as pay any legal fees and damages in the event a claim made is against you.

A **breach coach** who will guide you through the legal process of navigating a breach under attorney-client privilege. The coach will tell you what to report and when.

Business Income loss coverage for lost revenue due to an inability to use data/information that has been corrupted or deleted by an attack or malware.

A team of **marketing and public relations** consultants to help manage your organization's reputation in the wake of a breach.

A **forensic investigations** team to help you determine the size and scope of the breach and help get your business up and running again.

Provisions in the event that you have to pay ransom to a third-party or experience monetary loss due to a social engineering scam.

To be clear, cyber insurance isn't a replacement for cybersecurity. You should still invest in preventative measures to reduce the risk of a breach. But in case that's not enough, insurance will provide you with the resources and support you need to get your business back online and regain your clients' trust.

THE FUTURE IS CLOUD

Experts say that by 2021, cloud data centres will process 94% of workloads.⁴⁴ According to IDC, by 2024, 90% of enterprises will have multicloud strategies.⁴⁵ By 2025, the total amount of data in the world will quintuple and 49% of it will be stored in a public cloud environment.⁴⁶ More data combined with more clouds equates to incredibly complex digital environments for companies to manage.

Though the benefits of cloud—productivity, on-demand access, collaboration, scalability, and cost savings—are abundantly clear and easy to quantify, the risks remain a challenge. Organizations must implement clear cloud risk management strategies, understand their data protection responsibilities, and invest in both cyber security and cyber security insurance to adequately manage their exposures, or otherwise face the consequences.

Currently, 66% of enterprises have implemented “cloud excellence teams” which determine which applications are best suited to each cloud, optimize cloud costs, and set policies for cloud usage.⁴⁷ While SMBs likely do not have the resources to implement full-scale cloud teams, they can still make an effort to better understand risks and plan ahead, to truly realize the benefits of the cloud, worry-free.

44. “48% of corporate data is now stored on the cloud”, Panda, October 17, 2019, <https://www.pandasecurity.com/mediacenter/security/cloud-security-encryption/#>.

45. Frank Gens, et al., “IDC FutureScape, Worldwide IT Industry 2019 Predictions”, IDC, November, 2018, <https://www.idc.com/getdoc.jsp?containerId=WC20181030>.

46. “The Digitization of the World from Edge to Core,” *IDC White Paper, sponsored by Seagate*, November 2018, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.

47. “Cloud Computing Trends: 2019 State of the Cloud Survey”, *Flexera*, February 27, 2019, <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/>.

NEED GUIDANCE?

We will help you plan and protect. We can share what steps others in your industry are taking and advise you based on your unique operations. Our goal is to build resilient organizations.

We are PROLINK—Canada's Insurance Connection, a national insurance brokerage focused on building resilient organizations through insurance and risk management tools.

FOR ADVICE, PLEASE CONTACT:

PETER McCABE

Risk Advisor & Technology Practice Leader

PROLINK—Canada's Insurance Connection

T: 416 644 7730

E: PeterM@prolink.insure

VISIT OUR WEBSITE

We make the road to organizational resilience simpler.
So you can arrive where you need quicker.

WORKS CITED

1. "48% of corporate data is now stored on the cloud." *Panda*. October 17, 2019. <https://www.pandasecurity.com/mediacenter/security/cloud-security-encryption/#>.
2. "2019 CIRA Cybersecurity Survey." *CIRA*. Accessed March 4, 2020. <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>.
3. "2019 Cost of a Data Breach Report." *IBM Security*. Accessed March 14, 2020. <https://databreachcalculator.mybluemix.net/executive-summary>.
4. "Businesses collect more data than they can handle, reveals Gemalto." *Gemalto*. July 10, 2018. <https://www.gemalto.com/press/pages/businesses-collect-more-data-than-they-can-handle-reveals-gemalto.aspx>.
5. "CANADA | GLOBAL THREAT REPORT | DEFENDER POWER ON THE RISE." *Carbon Black. Canada*. October, 2019. <https://www.carbonblack.com/resources/threat-research/thank-you-45385/>.
6. "Canadians deserve a better internet." *CIRA*. Accessed March 4, 2020. <https://www.cira.ca/resources/state-internet/report/canadians-deserve-a-better-internet>.
7. "Cloud Computing Trends: 2019 State of the Cloud Survey." *Flexera*. February 27, 2019. <https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/>.
8. "Cloud market share Q4 2019 and full-year 2019." *Canalys*. February 4, 2020. https://www.canalys.com/static/press_release/2020/Canalys---Cloud-market-share-Q4-2019-and-full-year-2019.pdf.
9. "Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report." *McAfee*. 2019. <https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/rp-cloud-adoption-risk-report-iaas.pdf>.
10. "Cloud Security Report." *Cybersecurity Insiders*. 2019. <https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/>.
11. Columbus, Louis. "83% Of Enterprise Workloads Will Be In The Cloud By 2020." *Forbes*. January 7, 2018. <https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#76eeabe46261>.
12. Dosal, Eric. "7 Cloud Security Challenges and Risks to Be Aware Of." *Compuquip Cyber Security (blog)*. March 5, 2020. <https://www.compuquip.com/blog/cloud-security-challenges-and-risks>.
13. "Driving growth together: Small businesses and the cloud." *Office 365*. Accessed March 14, 2020. <https://info.microsoft.com/rs/microsoftdemandcenter/images/driving-growth-together-small-businesses-and-cloud-infographic.pdf>.
14. Gens, Frank., Gillen, Al., Mohan, Deepak., Nadkarni, Ashish., Palmer, Robert., Pike, Sean., Schubmehl, David., Villars, Richard L., Wester, James. "IDC FutureScape, Worldwide IT Industry 2019 Predictions." *IDC*. November, 2018. <https://www.idc.com/getdoc.jsp?containerId=WC20181030>.
15. Goasduff, Laurence. "Why Organizations Choose a Multicloud Strategy." *Gartner*. May 7, 2010. <https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy>.
16. Hou, Tony. "IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More." *Big Commerce (blog)*. Accessed March 9, 2020. <https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-key-differences-between-on-premise-saas-paas-iaas>.
17. Leber, Dennis. "Behind The Data Breach: Understanding Cloud Security And Misconfigurations." *Cyber Security Hub*. September 17, 2019. <https://www.cshub.com/cloud/articles/behind-the-data-breach-understanding-cloud-security-and-misconfigurations#>.
18. Mayaan, Gilad (GiladMayaan). "Top Cloud Data Security Challenges and How to Overcome Them." *IBM Developer*. September 20, 2019. <https://developer.ibm.com/recipes/tutorials/top-cloud-data-security-challenges-and-how-to-overcome-them/>.
19. Miteva, Ani. "8 cloud adoption statistics that reveal the future of the cloud." *Cloud Worldwide Services*. March 20, 2018. <https://www.cloudworldwideservices.com/en/cloud-adoption-statistics-cloud-future/>.
20. Panetta, Kasey. "Is the Cloud Secure?." *Gartner*. October 10, 2019. <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>.
21. Pedigo, Chris. "The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020." *Lacework (blog)*. December 13, 2019. <https://www.lacework.com/top-cloud-breaches-2019/>.
22. Rundle, James. "Human Error Often the Culprit in Cloud Data Breaches." *Wall Street Journal*. August 27, 2019. <https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203>.
23. "The Digitization of the World from Edge to Core." *IDC White Paper sponsored by Seagate*. November, 2018. <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.
24. "What Is a Public Cloud? | Public Cloud vs. Private Cloud." *Cloudflare*. Accessed March 6, 2020. <https://www.cloudflare.com/learning/cloud/what-is-a-public-cloud/#>.
25. Wilson, Victoria. "10 Cloud Computing Statistics You Need To Know." *Sys Group*. Accessed March 3, 2020. <https://www.sysgroup.com/resources/blog/10-cloud-computing-statistics-2018>.
26. "Worldwide Public Cloud Services Spending Forecast to Reach \$210 Billion This Year, According to IDC." *IDC*. February 28, 2019. <https://www.idc.com/getdoc.jsp?containerId=prUS44891519>.
27. Zeilman, Timothy. "Is your data in the cloud? It's still at risk of cyberattack." *NU Property Casualty 360*. February 28, 2019. <https://www.propertycasualty360.com/2019/02/28/is-your-data-in-the-cloud-its-still-at-risk-of-cyberattack/?slreturn=20200214214758>.

