International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 06 June 2022

DOI: 10.47191/ijsshr/v5-i6-08, Impact factor- 5.871

Page No: 2050-2065

Given the January 6, 2021 Riot and the Parler Debacle, is Cloud Computing a Riskless Cyber Medium When Conducting Risk Assessments and Key Risk Indicator Calculations?

Donald L. Buresh, Ph.D., J.D., LL.M.
Morgan State University

ABSTRACT: This essay aims to discuss the low probability of occurrence and high probability of impact risk introduced into the business risk equation when the cloud computing services that Parler Corp. contracted from Amazon.com, Inc. In a few days, Parler was pulled from the Google Play Store and the Apple Store. Because of these actions of its cloud computing providers, Parler went from a company valued at $1 billion to an organization that was effectively broke and unable to do business. The acts of Amazon, Apple, and Google demonstrated the immense power yielded by cloud computing providers over the business activities of their customers. Companies should be mindful that when engaging the services of a cloud computing provider, they are exposing the business to an unacceptable level of risk. A firm should evaluate this risk and decide whether it is worth assuming. An organization ignores this risk at its peril.

KEYWORDS: Cloud Computing January 6, 2021 Riot, Key Performance Indicators, Key Risk Indicators, Parler Corp, Risk Assessments, Risk Factors

INTRODUCTION

On January 6, 2021, protesters entered the halls of Congress as people were climbing the outside walls of the building and rushing the doors. The people entered the building, intent on confronting the members of Congress that Joseph Biden and the Democratic Party stole the November 3, 2020 election from Donald Trump and the Republican Party.[1] [2] For a period of time, it was chaos in the building. A Capital police officer fatally shot Ashli Babbitt while a stampede of fellow rioters crushed Rosanne Boyland. Kevin D. Greeson died of a heart attack, and Benjamin Philips died of a stroke. Capital Officer Brian D. Sicknick, an individual who was attacked by the mob, died the next day. Officer Jeffrey Smith of the Metropolitan Police and Officer Howard S. Liebengood of the Capital Police committed suicide, allegedly because of the riot.[3]

Days after the event, it was determined that the protestors had used Parler, a free speech social network alternative to Twitter and Facebook, was effectively driven out of business when it was unable to host its services.[4] The crushing of Parler by the cloud computing providers has introduced a new risk into the business equation of storing corporate data on the cloud. What happens if successful business suddenly loses its ability to access its data due to the machinations of a fickle cloud computing provider? What occurs if a viable company runs afoul of the policies of a cloud computing provider merely because it has different values than the provider? If the cloud computing provider suddenly withdraws its services with little to no notice, a firm could be out of business overnight. It is this low probability, high impact risk that this paper is attempting to explore.

[1] Erin Doherty, & Oriana Gonzalez, In photos: An hour-by-hour record of the Jan. 6 Capitol riot, Axios (Jan. 6, 2022), available at https://www.axios.com/capitol-riot-january-6-anniversary-c61435e4-f4c4-4f5a-b6d1-9c463ac7eed2.html.

[2] *See generally*, Thomas Dreisbach, Meg Anderson, & Barbara van Woerkom, *5 Takeaways from the Capitol Riot Criminal Cases, One Year Later*, NATIONAL PUBLIC RADIO (Jan. 5, 2022), *available at* https://www.npr.org/2022/01/05/1070199411/5-takeaways-from-the-capitol-riot-criminal-cases-one-year-later.

[3] Chris Cameron, *These Are the People Who Died in Connection With the Capitol Riot*, THE NEW YORK TIMES (Jan. 5, 2022), *available at* https://www.nytimes.com/2022/01/05/us/politics/jan-6-capitol-deaths.html.

[4] Jack Nicas, &^ Davey Alba, *Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters*, THE NEW YORK TIMES (Jan. 9, 2021), *available at* https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html.

Given the January 6, 2021 Riot and the Parler Debacle, is Cloud Computing a Riskless Cyber Medium When Conducting Risk Assessments and Key Risk Indicator Calculations?

Risk Assessments

How can one convince an organization that a risk assessment simulation is worth the effort? Risk analysis has a cost because it takes time and effort to create the culture, processes, and tools to perform effectively and efficiently. The issue is that the benefits are frequently difficult to discern, and the more critical benefits are usually not noticeable.[5]

First, risk analysis is a thinking exercise because it allows a team to scrutinize a risk assessment plan and ask the following three questions:

- What could occur?
- What is the impact?
- How can the risk be mitigated?

Risk analysis allows an organization to identify risk events, determine how the risks impact the entity, and investigate the optimal way to minimize the impact. Risk analysis encourages thinking and communication, which are keys to successful endeavors.[6]

Second, one of the most effective ways to evaluate an entity's security is to develop a risk assessment adjusted by cost and schedule so that a margin of error is present in determining the confidence of success.[7] Risk can usually be divided into two categories – risk events that are manageable and risk events that are uncertain. Risk events that can be managed can be avoided, transferred, mitigated, or accepted, depending on their expected impact. These risk events can only be minimized. They cannot be eliminated. However, what remains are residual risks that should be accounted for. When addressing uncertain risks, a firm needs to account for uncertainty, which is the variance of all activities within an organization. The uncertainties can be characterized as statistical distributions (e.g., beta, normal, etc.) with probability distributions.[8]

The level of uncertainty may depend on personnel, technology maturity, and development type. An adjusted risk assessment plan can be generated by assigning risks and uncertainties to corporate activities and the running Monte Carlo simulations. This plan guides an organization on the level of risk and the risk appropriateness schedules and cost contingencies.[9]

Monte Carlo simulation has significant limitations. In many instances, software applications cannot distinguish between variability and uncertainty.[10] For example, body weight and drinking water are notable differences among individuals and variability. On the other hand, frequency and duration are usually unknown and constitute uncertainty. Monte Carlo techniques typically treat uncertainty as variability, generating misleading results. Issues and limitations with simulation include:

- Simulations cannot distinguish between variability and uncertainty;
- Simulations ignore correlations among variables that can bias Monte Carlo calculations; and
- Short-term exposure factors may not accurately represent long-term-conditions.

Because of these limitations, a Monte Carlo simulation may not be the best or even the primary risk assessment method. Even so, Monte Carlo simulations typically yield superior results to qualitative procedures when analyzing variability and uncertainty.[11] Thus, the Monte Carlo method may be acceptable in developing corporate risk assessments.

Obtaining Risk Assessment Information

According to Mark Zuckerberg, founder of Facebook, "[t]he biggest risk is not taking any risk. In a world that's changing really quickly, the only strategy that is guaranteed to fail is not taking risks."[12] The risk assessment steps include:

- Identify the hazards;
- Determine who might be harmed and how;
- Evaluate the risks and take precautions;
- Record the findings; and
- Review the assessment and update when needed.[13]

With the risk assessment process, users examine an organization to:

---

[5] Intaver Staff, *What are the benefits of project risk analysis?*, INTAVER INSTITUTE (n.d.), *available at* https://intaver.com/blog-project-management-project-risk-analysis/benefits-project-risk-analysis/.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] EPA Staff, *Use of Monte Carlo Simulation in Risk Assessments: Use of Monte Carlo Simulation in Risk Assessments*, UNITED STATES ENVIRONMENT PROTECTION AGENCY (n.d.), *available at* https://www.epa.gov/risk/use-monte-carlo-simulation-risk-assessments.
[11] *Id.*
[12] Lucid Content Team, *A Complete Guide to the Risk Assessment Process*, LUCIDCHART (n.d.), *available at* https://www.lucidchart.com/blog/risk-assessment-process.
[13] *Id.*

- Recognize processes and situations that may result in harm;
- Determine the likelihood a hazard will occur and the severity of the consequences; and
- Select what actions should be taken to prevent a risk from occurring or decide to control the risk.[14]

There is a difference between hazards and risks. A hazard causes harm, including work accidents, emergencies, toxic chemicals, employee conflicts, and stress. On the other hand, a risk is a chance that a hazard will cause harm. In a risk assessment plan, hazards should be identified so that the risk value can be calculated.[15]

In obtaining information for a risk assessment, it is essential to ask the right people the right questions. In this author's opinion, it is the only way to quickly gather the information for a risk assessment at a meeting or any other gathering. Any other method lacks the urgency and clarity needed to collect accurate and precise risk assessment data. Typical questions that could be asked to obtain risk information are:

- What are the entity's most valuable assets?
- What are the perceived risks?
- What are the suggested strategies to mitigate the risks?
- What are the strengths and weaknesses of the firm's security system?
- What are the solutions to mitigate or eliminate these risks?
- What are the risk assessment products available to the company?
- How frequently should a firm reevaluate risks?[16]

Another set of questions to quickly gather risk assessment information are:

- What are the firm's most significant risks, impact, and likelihood?
- How frequently does a firm reassess its risks?
- Who is responsible for the company's most significant risks?
- How effective is the organization in managing its risks?
- Are there organizational blind spots demanding attention?
- Does the company appreciate the key assumptions of its risk strategy?
- Is the firm's risk strategy capable of changing based on external forces?
- Does the company have an explicit risk appetite and risk tolerance?
- Does the company's risk reporting mechanism provide the correct information to senior management and the board of directors?
- Are there opportunities to enhance the risk reporting process?
- Is there a process for monitoring and reporting emerging risks to senior management and the board of directors?
- Is the firm prepared to respond to extreme events?
- Does the company possess response plans for extreme events?
- Has the firm prioritized its high-impact, low-likelihood risks?
- Does the board have the necessary skill sets to ensure effective risk oversight?[17]

The first set of questions is general, whereas the second list of questions is quite specific. Specific questions must be asked to collect specific information. General questions can be asked, but the responses to these questions will likely be vague and possibly misleading. There is no royal road to gather information. Sometimes, a single or a few questions can be asked that will yield a treasure trove of information. However, these circumstances are few and far between, or the individual asking these insightful questions already has an intimate knowledge of the entity. These situations are rare.

SWOT Analysis

In this section, a SWOT analysis is defined, followed by a discussion of the components of a SWOT analysis. The third subsection deals with the relationship between A SWOT analysis and security controls.

[14] *Id.*
[15] *Id.*
[16] Edafio Staff, *7 Crucial Questions To Ask During A Security Risk Assessment*, EDAFIO TECHNOLOGY PARTNERS (n.d.), *available at* https://edafio.com/blog/7-crucial-questions-to-ask-during-a-security-risk-assessment/.
[17] Jim DeLoach, *10 Questions You Should Ask About Risk Management*, CORPORATE COMPLIANCE INSIGHTS (Feb. 18, 2018), *available at* https://www.corporatecomplianceinsights.com/ten-questions-you-should-ask-about-risk-management/.

Given the January 6, 2021 Riot and the Parler Debacle, is Cloud Computing a Riskless Cyber Medium When Conducting Risk Assessments and Key Risk Indicator Calculations?

DEFINITION OF SWOT

The acronym "SWOT" stands for "Strengths, Weaknesses, Opportunities, and Threats."[18] It is a framework used in strategic planning to assess internal and external factors, including an organization's current and future potential.[19] The purpose of a SWOT analysis is to provide a realistic, fact-based, data-driven examination of the strengths and weaknesses of an entity.[20] A SWOT analysis must avoid pre-conceived beliefs or assumptions by focusing on actual, real-life issues so that it may act as a guide rather than a prescription.[21]

Components of a SWOT Analysis

The main components of a strategic planning process begin with an organization's mission and goals.[22] An internal analysis of strengths and weaknesses and an external analysis of opportunities and threats feed into a SWOT analysis, where the output is a functional-level strategy, a business-level strategy, a global strategy, and a corporate-level strategy.[23] Implementing these strategies includes designing an organizational structure, designing control systems, and matching strategy, structure, and control to manage strategic change.[24] The three outputs can then be fed back into the organization's missions and goals, creating a positive feedback loop.[25] Pictorially, the strategic planning process looks like:

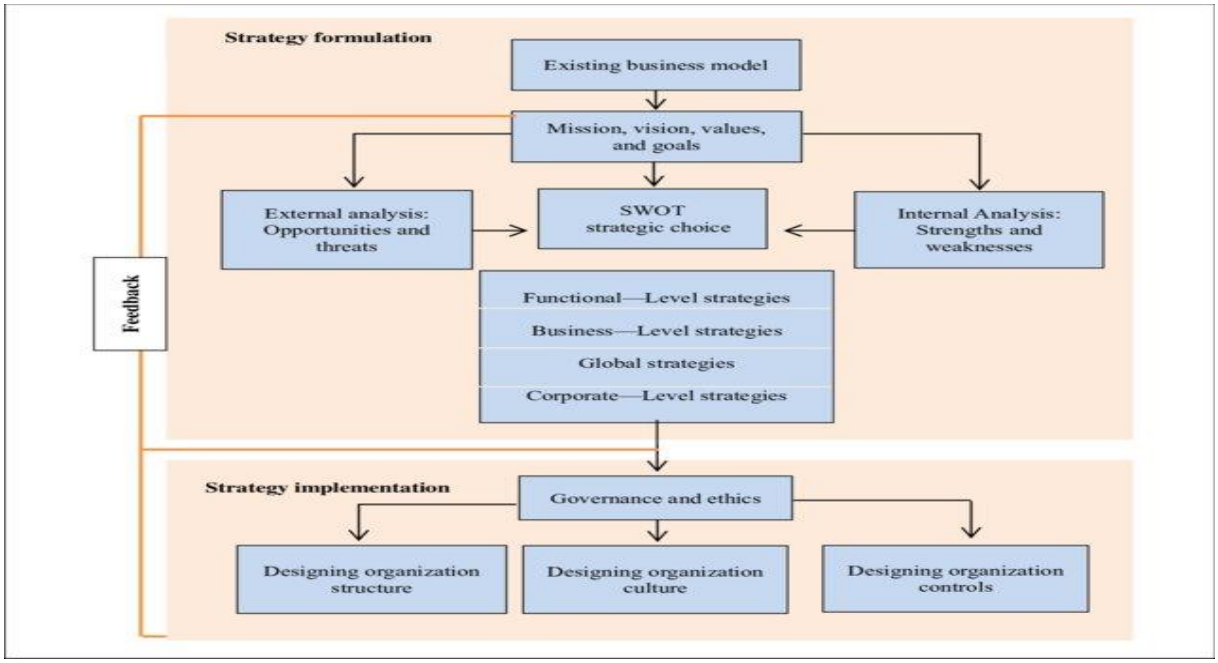

Figure 1. The Main Components of the Strategic Planning Process.[26] Reproduced with permission.

A corporate-level strategy is a guiding force behind a firm.[27] A corporate strategy sets priorities and shared goals, focuses on using resources, and specifies the expected results or achievement.[28] A global strategy is a strategy that an organization implements when it desires to expand into a global marketplace.[29] It is a strategy that targets growth beyond an entity's national borders to increase the sale of goods and services internationally.[30] Business-level strategies translate corporate-level strategies into tangible actions by

[18] Will Kenton, Gordon Scott, & Ariel Courage, *Strength, Weakness, Opportunity, and Threat (SWOT) Analysis*, INVESTOPEDIA (Updated Mar. 29, 2021), *available a*t https://www.investopedia.com/terms/s/swot.asp.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] CHARLES W. L. HILL, & GARETH R. JONES, STRATEGIC MANAGEMENT: AN INTEGRATED APPROACH 5 (Houghton Mifflin Company 1998).
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] Sling Staff, *Functional Level Strategy: What It Is Plus 18 Examples*, SLING (n.d.), *available at* https://getsling.com/blog/functional-level-strategy/.
[28] *Id.*
[29] Richard Lynch, *Global Strategy – Definition and Meaning*, MARKET BUSINESS NEWS (n.d.), *available at* https://marketbusinessnews.com/financial-glossary/global-strategy/.
[30] *Id.*

assigning the necessary activities to achieve the corporate-level strategy.[31] Business-level strategies include increasing the market budget, improving product quality, or broadening the organization's exposure to the relevant markets.[32] Finally, functional-level strategies are the actions and goals that are assigned to different departments that support business-level and corporate-level strategies.[33] Functional-level strategies establish the desired outcomes to be achieved from the daily operations of specific departments.[34] Functional-level strategies integrate multiple functional areas to achieve corporate and business objectives.[35] Examples include increased hiring of highly-trained individuals, improving brand identification, or reducing customer product rejections.[36]

SWOT and Security Controls

Given the characterization above, the question is: Where does security fit in a SWOT analysis? In a business, the three types of security are management security, operational security, and physical security.[37] Management security addresses corporate controls' overall design that provides the guidance, rules, and procedures for ensuring a secure environment.[38] Operational security deals with the effectiveness of the management controls, including access controls, authentication, and security topologies that apply to networks, systems, and applications.[39] Physical security protects personnel, data, and hardware from physical threats that can harm, damage, or disturb business operations by impacting the confidentiality, integrity, or availability of systems or data.[40] Based on the discussion above, when a SWOT analysis is applied to security, the inquiry focuses on business-level and function-level strategies because security is concerned with a business as a whole and its implementation on a functional level.

It should be remembered that a company is a mechanism for transforming inputs into outputs, where inputs consist of labor, land, capital (machines and not money), management, and technological know-how.[41] The equation that measures the efficiency of an organization is:

Efficiency = Outputs / Inputs (1)

where a firm is more efficient when it produces a given level of outputs using fewer inputs, this means that when security is evaluated, its effectiveness should be measured by how its existence improves the efficiency of an organization. From a SWOT perspective, security must be gauged on its ability to promote competitive advantage[42] so that an entity provides more excellent shareholder value.[43] One could also argue that security from a SWOT viewpoint should improve stakeholder value, where a stakeholder is a "party that has an interest in a company and can either affect or be affected by the business," such as investors, employees, customers, and suppliers.[44]

GAP ANALYSIS

In this section, gap analysis is explained. The first and second subsections define gap analysis and describes how gap analysis is applied respectively. The third subsection highlights the McKinsey 7-S framework followed by the Nadler-Tushman Congruence Model. The fourth subsection compares the two analysis frameworks, noting the similarities and differences.

DEFINITION OF GAP ANALYSIS

Gap analysis is defined as a "method of assessing the performance of a business unit to determine whether business requirements or objectives are being met and, if not, what steps should be taken to meet them."[45] Needs analysis, needs assessment, or need-gap

[31] Sling Staff, *supra*, note 27 .
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] Brian Willis, *Three Categories of Security Controls*, LMBC FAMILY OF COMPANIES (n.d.), *available at* https://www.lbmc.com/blog/three-categories-of-security-controls/.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] Charles W. L. Hill, & Gareth R. Jones, *supra*, note 23 at 144.
[42] MICHAEL E. PORTER, COMPETITIVE ADVANTAGE: CREATING AND SUSTAINING SUPERIOR PERFORMANCE (The Free Press 1985).
[43] *Dodge v. Ford Motor Company*, 204 Mich. 459, 170 N.W. 668 (Mich. 1919) (here, the court opined that the purpose of a company is to maximize shareholder value).
[44] Jason Fernando, Thomas Block, & Pete Rathburn, *Stakeholder*, INVESTOPEDIA (Aug. 19, 2021), *available at* https://www.investopedia.com/terms/s/stakeholder.asp.
[45] Katie Terrell Hanna, & Francesca Sales, *Gap Analysis*, TECHTARGET (Oct. 2021), *available at* https://www.techtarget.com/searchcio/definition/gap-analysis.

analysis are other names for a gap analysis.[46] The so-called "gap" in gap analysis is the variance, difference, or space between where an organization is currently (the present state) and where it wants to be (the target or desired state).[47]

APPLICATION OF GAP ANALYSIS

Corporate performance gaps can be identified and measured from different perspectives, including customer satisfaction, revenue generation, supply chain costs, and even security.[48] In software development and security, gap analysis tools can record what tangible and intangible assets have been accidentally ignored or under-protected.[49] When dealing with a security framework, a gap analysis can be employed to compare what is required or needed versus the entity's current state. With security, one can examine what security controls are present within an organization versus what a security framework states should and ought to exist. In performing a gap analysis, it should be remembered that the point of the gap analysis is to improve the competitiveness and efficiency of the firm, where outputs divided by inputs measure efficiency.[50]

The following are the four steps in a gap analysis:

- Establish specific target objectives by evaluating a firm's mission statement, business goals, and improvement objectives;
- Analyze current processes by gathering performance data;
- Evaluate the allocation of resources;
- Compare target objectives against the current processes and resource allocations; and
- Develop a comprehensive plan to transform an entity from its current state to its desired state.[51]

The final step is known as strategic planning, as identified by Hill and Jones.[52]

Types of Gap Analyses

According to Hanna and Sales, the three types of gap analyses are the McKinsey 7-S Framework, the Nadler-Tushman Congruence Model (NTCM), and SWOT analysis.[53] A SWOT analysis has been previously discussed above, so it will not be covered again.

MCKINSEY 7-S FRAMEWORK

The McKinsey 7-S Framework was generated in the late 1970s by Tom Peters and Robert Waterman, both former consultants at McKinsey & Company. Peters and Waterman identified seven internal elements within an organization that should be aligned to ensure success.[54] The model characterizes the seven elements as either hard or soft. The three hard elements are strategy, structure (hierarchal organizational charts), and systems (IT systems and other formal processes).[55] The four soft elements include shared values, skills, style, and staff. These elements are more difficult to define yet are a critical part of the framework.[56]

Individually, the elements are:

- Strategy – An organization's plan for building and maintaining a competitive advantage over its competitors;
- Structure – The organization of the company and who reports to who;
- Systems – The daily activities and procedures performed by the staff to perform their jobs;
- Shared Values – The core values of the organization, reflecting its general work ethic;
- Style - The style of the company's leadership;
- Staff – The employees and their general capabilities; and
- Skills – The employee's skills and competencies.[57]

[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] Charles W. L. Hill, & Gareth R. Jones, *supra*, note 23.
[51] Katie Terrell Hanna, & Francesca Sales, *supra*, note 45.
[52] Charles W. L. Hill, & Gareth R. Jones, *supra*, note 23.
[53] Katie Terrell Hanna, & Francesca Sales, *supra*, note 45.
[54] Mind Tools Content Team, *McKinsey 7-S Framework: Making Every Part of Your Organization Work in Harmony*, MIND TOOLS (n.d.), *available at* https://www.mindtools.com/pages/article/newSTR_91.htm.
[55] *Id.*
[56] *Id.*
[57] Id.

Shared values are at the center of the module because they are central to the development of the other elements.[58] The framework advocates that the seven elements should balance and reinforce each other to ensure that the organization operates effectively and efficiently.[59]

NADLER-TUSHMAN CONGRUENCE MODEL

The NTCM was developed in the 1980s by David A. Nadler and Michael L. Tushman.[60] The model aims to identify the root causes of organizational performance issues and how these issues can be modified to ensure optimal efficiency.[61] The model's premise is that team or an organization can only succeed when the organizational structure and the culture fit together.[62]

The NTCM is an input-process-output model, where the inputs consist of an entity's strategy, resources, and environment, while the outputs are made up of the organizational, team, and individual performance.[63] The four processes of the model are culture, people, structure, and work.[64]

When applying the NTCM, the following three steps should be taken:

- Analyze the culture, structure, people, and work, each one separately;
- Understand the relationships between an organization's culture, structure, people, and work; and
- Build and sustain unity among the elements.[65]

There are limitations to the NTCM. First, NTCM is a tool for analyzing team or organizational issues but cannot be used to rectify an issue.[66] Second, NTCM does not recommend the best culture, the best structure, the best people, or the best work.[67] Other tools must be employed to obtain the desired result. Finally, NTCM focuses on an entity's internal environment but does not deal with external corporate issues.[68]

COMPARISON OF GAP ANALYSES

When comparing the three gap analysis techniques as discussed by Hanna and Sales, the thing that stands out is that the McKinsey 7-S Framework and the Nadler-Tushman Congruence Model are both internal mechanisms to promote an efficient organization. The McKinsey 7-S Framework can help an entity improve performance when experiencing restructuring, new processes, organizational mergers, new systems, and a leadership change.[69] However, when a firm faces external opportunities or threats, the framework speaks volumes with its silence. The McKinsey 7-S Framework does not address external opportunities or threats in any meaningful way,

The Nadler-Tushman Congruence Model is even more restrictive. Its purpose is to identify areas where greater performance and efficiency can be achieved but cannot modify internal performance issues when identified.[70] This is a severe limitation of the model. However, the NTCM can be employed in helping expose the strengths and weaknesses of an organization but is powerless in aiding an organization devoted to transforming its strategy when confronted with external opportunities and threats. Only a SWOT analysis can accomplish both arduous labors maximizing internal strengths and minimizing weaknesses while ascertaining external opportunities and pinpointing threats. Thus, a SWOT analysis is the most comprehensive of the three gap analysis techniques.

When the three gap analysis techniques are viewed from a security perspective, all three techniques have value. The three techniques can be used to identify internal security issues because internal issues play into their strengths. The McKinsey 7-S Framework may act as a basis for alleviating security issues, but a company is better served by employing a particular security framework, such as NIST 800-53, the Cybersecurity Framework, ISO 27001-27002, or any of the numerous other industry-specific frameworks. The NTCM suffers from the same limitations as the McKinsey 7-S Framework.

A SWOT offers the most significant promise when dealing with security issues. However, it is a general-purpose methodology not designed to address specific security concerns. Thus, even when employing a SWOT analysis, a company is better

[58] *Id.*
[59] *Id.*
[60] Mind Tools Content Team, *The Nadler-Tushman Congruence Model: Aligning the Drivers of High Organizational Performance*, MIND TOOLS (n.d.), *available at* https://www.mindtools.com/pages/article/newSTR_95.htm.
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Mind Tools Content Team, *supra*, note 54.
[70] Mind Tools Content Team, *supra*, note 60.

served by using one of the several security frameworks listed above. Only then can a firm be satisfied that it has dealt with security needs in protecting personal information, software, and hardware assets.

KEY RISK INDICATORS

This part of the essay discusses key risk indicators (KRIs). First, a KRI is defined, followed by a description of a KRI. Several examples of KRIs are provided, and key performer indices (PKIs) are shown not to be KRIs. The challenges associated with KRI are outlined. Then, risk metrics and risk measures are defined, and examples are given. Finally, KRIs are revisited. The essay concludes by observing that KRIs are more than risk metrics and measures. KRIs are quantifiable, measurable, able to be validated, and relevant to the success of a business.

KEY RISK INDICATOR DEFINITION

According to TechTarget, a KRI is a "metric for measuring the likelihood that the combined probability of an event and its consequences will exceed the organization's risk appetite and have a profoundly negative impact on its ability to be successful."[71] The benefits of KRIs include:

- Advance notice of potential risks that could damage an entity;
- Discernment into possible weaknesses in monitoring and control tools; and
- Continuing risk monitoring via periodic risk assessments.[72]

CHARACTERISTICS OF A KEY RISK INDICATOR

The characteristics of a reasonable and measurable KRI are as follows:

- Contains details on the people, processes, technologies, facilities, and other corporate attributes that are most important to the organization's continued operation and success;
- Identifies risks, threats, and vulnerabilities the organization faces based on their likelihood of occurring, their operational and financial impact to the firm, and the firm's ability to mitigate the event;
- Ranks the business attributes in terms of their criticality to the firm;
- Ranks risks, threats, and vulnerabilities in terms of their potential harm to the firm;
- Connects key business attributes to the most significant risks to identify those issues of greatest concern to the organization;
- Identifies when and how an identified risk becomes a serious threat to critical attributes of the organization;
- Encourages a firm to review KRIs and their metrics to identify any changes that require management review and possible action; and
- Has been approved by senior management.[73]

Good KRIs should be quantifiable, measurable, validated, and relevant.[74]

Examples of a Key Risk Indicator

Examples of KRIs are contained in the table below:[75]

Table 1. Examples of Key Risk Indicators

Type of KRI	Risk Situation	Suggested KRI	Measurement
People	Turnover	Identify when employee turnover exceeds a certain level	The total annual turnover rate exceeds 30 percent
People	Employee frustration	Identify situations that demonstrate employee frustration	The number of employee complaints increases by 20 percent or more quarterly
Process	Production of the firm's primary product does not meet the demand	Identify when production levels attain the productive capacity	The number of daily units produced is 20 percent less than orders received

[71] TechTarget Staff, *Key Risk Indicator (KRI)*, TECHTARGET (Oct. 2021), *available at* https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI.
[72] *Id.*
[73] *Id.*
[74] SolveXia Staff, *Key Risk Indicators: Examples and Definitions*, SOLVEXIA (Dec. 15, 2020), *available at* https://www.solvexia.com/blog/key-risk-indicators.
[75] TechTarget Staff, *supra*, note 71.

Process	Product design does consider current market trends	Based on sales risk statistics, decide when to change existing products	Product sales have decreased by 25 percent or more from previous levels
Technology	IT network systems are victims of cyber attacks	Determine the best latch level for the IT system	An IT system is three patches behind the recommended patch levels
Technology	Cannot recover systems, data files, and databases after a disaster because backups are corrupted	A metric showing that the backup levels are current	Backup systems alert IT staff, when backup levels are more than one week old

KRIs are important because without them, the probability of an organization being subjected to events or situations that could damage a business increases.[76] In other words, KRI is the red flag that warrants that risks are recognized in advance and then mitigated if they occur. The critical issue for an entity is to acknowledge which risk indicators are the most important so that everyone in an organization appreciates the significance of the risk indicator and responds accordingly.[77]

KEY PERFORMANCE INDICATORS

KRIs are not KPIs. A KPI assists a firm in assessing its progress towards its specified goals.[78] KRIs and KPIs are inverses of each other.[79] They are separate and distinct, but the generation of one often results in the creation of the other as its complement.[80] KRIs act as an early warning system for monitoring, analyzing, managing, and mitigating key risks.[81] In contrast, KPIs show how well an entity performs concerning goals and objectives, such as sales, revenues, or customer satisfaction.[82] Like KRIs, KPIs can be applied to people, processes, and technologies.[83]

Challenges with Key Risk Indicators

KRIs must be periodically monitored and reviewed to identify possible changes in a business, risk or threat levels, and any remedial action needed. Challenges with a KRI include:

- Obtaining accurate information to pinpoint mission-critical activities;
- Identifying risks, threats, and vulnerabilities, and then quantifying their probability, severity, and impact;
- Securing senior management support for employing KRIs in an enterprise risk management program;
- Linking critical business characteristics with probable risk scenarios;
- Creating measurable and understandable metrics;
- Establishing activities that monitor, measure, and analyze changes in metrics;
- Creating responses to KRIs in the presence of deviations.[84]

Risk Metrics and Risk Measures

When measuring risks, a risk measure is "the operation that assigns a value to a risk," whereas a risk metric is "the attribute of risk that is being measured."[85] According to Holton, the two components of risk are exposure and uncertainty.[86] For example, if an individual swims in a part of an ocean infested with sharks, they are exposed to a shark attack, but they may be uncertain if they will be attacked.[87] Risk metrics may quantify exposure, uncertainty, or both.[88] For example, the probability of snow is a risk metric that quantifies uncertainty, and it does not consider the exposure to snow.

[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] GLYN A. HOLTON, VALUE AT RISK: THEORY AND PRACTICE (Academic Press 2003).
[86] *Id.*
[87] *Id.*
[88] *Id.*

In contrast, credit exposure is a risk metric that quantifies exposure by indicating how much money a person would if a default occurred.[89] It says nothing about the uncertainty of whether a default will occur. Risk metrics that quantify both uncertainty and exposure are probabilistic with a probability distribution function.[90] For example, average highway deaths per mile quantify uncertainty and exposure.[91]

Key Risk Indicators Revisited

As can be readily seen from the KRIs in Table 1, the specified KRIs are neither solely risk metrics nor risk measures. They are much more than that. A KRI is a metric because it addresses uncertainty and exposure. It is a measure because it is quantifiable. However, a KRI can be validated and relevant to an organization. Thus, a KRI is much more than a mere measurable risk metric.

A key risk indicator is not merely a risk metric or a measure, although it possesses characteristics of both of these notions. The examples provided in Table 1 are KRIs because they are quantifiable, measurable, can be validated, and are relevant when running a successful business. A KRI is essential to ensure that adverse events are quickly identified and then appropriately mitigated so that a firm maximizes its profits, minimizes its costs, and maximizes shareholder value. It is as simple as that.

ISSUES WITH CLOUD COMPUTING

In this section, cloud computing is defined. In the next subsection, cloud computing is examined in light of the Parler Corp. (Parler) debacle. Parler is a free speech social network that lost its ability to do business when the major cloud computing providers refused to host its content. The following subsection assesses the risks of a corporation employing cloud computing to store company data and personal information. Three risk factor formulas are described, highlighting the advantages and disadvantages. In the final subsection, cloud computing is compared and contrasted with on-site computing, noting its advantages and disadvantages.

Cloud Computing Definition

According to Frankenfield, cloud computing is "the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software."[92] The idea behind cloud computing is that instead of storing files on a proprietary system, cloud-based storage permits individuals and businesses the ability to store data and software on the Internet.[93] Cloud computing is popular because of cost savings, increased productivity, speed and efficiency, performance, and security.[94]

TechTarget observes that cloud computing is a "general term for anything that delivers hosted services over the Internet. These services are divided into three main categories or types of cloud computing: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS)."[95] A cloud can be public or private, and sells its services to any individual or business on the Internet.[96] A private cloud is a "proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings."[97] Cloud computing aims to permit easy and scalable access to computing resources and other IT services.[98] Cloud computing can be considered utility computing or on-demand computing.[99]

Cloud Computing and Parler Corp.

Based on the discussion above, cloud computing could be construed as manna from heaven, where computing has been reduced to a utility accessible to just about everyone at a relatively low cost. The issue with this idealized perspective of cloud computing is that it seems too good to be true. And, as an adage aptly points out, something that is too good to be true is usually not true. The proponents of cloud computing seem to be lauding praises on cloud computing without ever considering its disadvantages. It should be remembered that every human activity, no matter what that activity may be, has advantages and disadvantages. Its advantages are widely acclaimed in cloud computing, while its disadvantages are seemingly ignored.

---

[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] Jake Frankenfield, & Julia Mansa, *Cloud Computing*, INVESTOPEDIA (Jul. 28, 2020), *available at* https://www.investopedia.com/terms/c/cloud-computing.asp.
[93] *Id.*
[94] *Id.*
[95] TechTarget Staff, *Cloud Computing*, TECHTARGET (Dec. 2021), *available at* https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*

Given the January 6, 2021 Riot and the Parler Debacle, is Cloud Computing a Riskless Cyber Medium When Conducting Risk Assessments and Key Risk Indicator Calculations?

Parler Corp. (Parler)is a free speech social network alternative to Twitter and Facebook. In August 2018, Parler was founded by John Matze Jr. and Jared Thomson in Henderson, Nevada.[100] The name of the company is French, meaning "to speak."[101] Parler quickly became the darling of political conservatives and alt-right individuals and groups.[102] [103] According to the company, Parler quickly attracted users, and at the beginning of January 2021, the firm had nearly 15 million users.[104]

According to Timberg and Hartwell, Parler was used in planning January 6, 2021, riot at the United States Capitol building.[105] [106] On January 2, 2021, Parler informed the Federal Bureau of Investigation (FBI) that its attorneys found material on its website that declared that on January 6, 2021, people would be taking a final stand, drawing a red line on Capitol Hill.[107] On January 5, 2021, the Secret Service notified the Capitol Police about an individual who attended the rally on January 6, 2021, intending to incite violence against the police.[108] Four hours before the riot, the phrase "civil war" increased four-fold on Parler.[109] Then January 6, 2021, a riot at the United States Capitol occurred. BuzzFeed observed that after the riot, Parler was flooded with death threats, support for violence, and calls to partake in another armed march in Washington, DC, on January 19, 2021, the day before Joseph Biden was sworn in as President of the United States.[110]

On January 8, 2021, Google pulled Parler from the Google Play Store, claiming that Parler posed a threat to public safety because of its apparent lack of moderation policies and enforcement.[111] Also, on January 8, 2021, Apple Computer, Inc. (Apple) required Parler to submit a moderation improvement by January 9, 2021 (24 hours) or be removed from the Apple Store. Although Parler complained that it was being pressured, the company failed to give Apple its moderation plan, and on January 9, 2021, Parler was removed from the Apple Store.[112] On January 9, 2021, Amazon.com, Inc. (Amazon) declared that it would suspend Parler from Amazon Web Services effective January 10, 2021, at 11:59 p.m. Pacific Time.[113] One minute later, at midnight, Parler went

[100] Alexis Benveniste, & Kaya Yurieff, *Meet Rebekah Mercer, the Deep-Pocketed Co-Founder of Parler, a Controversial Conservative Social Network*, CABLE NEWS NETWORK (CNN) (Nov. 16, 2020), *available at* https://www.cnn.com/2020/11/15/media/rebekah-mercer-parler/index.html.

[101] Mark Di Stefano, Alex Spence, & Ryan Mac, *Pro-Trump Activists Are Boosting a Twitter App Used by Banned Personalities and It Appears to Have Already Stalled*, BUZZFEED NEWS (Feb. 12, 2019), *available at* https://www.buzzfeed.com/markdistefano/pro-trump-activists-are-boosting-a-twitter-app-for-banned.

[102] Isaac Saul, *This Twitter Alternative Was Supposed to Be Nicer, but Bigots Love It Already*, FORWARD: JEWISH, INDEPENDENT, NON-PROFIT (Jul. 18, 2019), *available at* https://forward.com/news/427705/parler-news-white-supremacist-islamophobia-laura-loomer/.

[103] Brian C. Parker, *I Tried Parler, the Social Media App Where Hate Speech Thrives*, CHRON ()Dec. 01, 2020), *available at* https://www.chron.com/news/article/I-tried-Parler-the-social-media-app-where-hate-15765465.php.

[104] Keach Hagey, & Jeff Horwitz, *Parler, a Platform Favored by Trump Fans, Struggles for Survival*, THE WALL STREET JOURNAL (Jan. 11, 2021), *available at* https://www.wsj.com/articles/parler-struggles-survival-amazon-lawsuit-trump-fans-11610414745.

[105] Craig Timberg, & Drew Harwell, *Pro-Trump Forums Erupt with Violent Threats Ahead of Wednesday's Rally Against the 2020 Election*, THE WASHINGTON POST (Jan. 5, 2021), *available at* https://www.washingtonpost.com/technology/2021/01/05/parler-telegram-violence-dc-protests/.

[106] Sheera Frenkel, *The Storming of Capitol Hill Was Organized on Social Media*, THE NEW YORK TIMES (Jan. 6, 2021), *available at* https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html.

[107] Aaron C. Davis, *Red Flags*, THE WASHINGTON POST (Oct. 31, 2021), *available at* https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/.

[108] Betsy Woodruff Swan, & Nicholas Wu, *Secret Service Warned Capitol Police About Violent Threats 1 Day before Jan. 6*, POLITICO (Aug. 25, 2021), *available at* https://www.politico.com/news/2021/08/25/secret-service-warned-capitol-police-violent-threats-january-riot-506806.

[109] Aleszu Bajak, Jessica Guynn, & Mitchell Thorson, *When Trump Started His Speech Before the Capitol Riot, Talk on Parler Turned to Civil War*, USA TODAY (Feb. 1, 2021), *available at* https://www.usatoday.com/in-depth/news/2021/02/01/civil-war-during-trumps-pre-riot-speech-parler-talk-grew-darker/4297165001/.

[110] John Paczkowski, & Ryan Mac, *Amazon Will Suspend Hosting for Pro-Trump Social Network Parler*, BUZZFEED NEWS (Jan. 9, 2021), *available at* https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws.

[111] Ashley Gold, & Shawna Chen, *Google Suspends Parler from App Store After Deadly Capitol Violence*, AXIOS (Jan. 8, 2021), *available at* https://www.axios.com/capitol-mob-parler-google-ban-826d808d-3e06-4468-a7c6-6157557818b3.html.

[112] Emma Bowman, *Amazon and Apple Drop Parler*, NATIONAL PUBLIC RADIO (NPR), (Jan. 9, 2021), *available at* https://www.npr.org/2021/01/09/955329265/amazon-and-apple-drop-parler.

[113] Annie Palmer, *Amazon Drops Parler from Its Web Hosting Service, Citing Violent Posts*, CNBC (Jan. 9, 2021), *available at* https://www.cnbc.com/2021/01/09/amazon-drops-parler-from-its-web-hosting-service.html.

offline.[114] Although Parler sued Amazon for anti-trust violations, the court ruled in Amazon's favor.[115] Parler then filed a defamation and breach of contract suit in state court.[116]

On January 17, 2021, Parler came back online with a static webpage and no functionality.[117] The service returned online for existing users on February 15, 2021, with a new website and logo, and where postings before February 15, 2021, were no longer available.[118] Parler announced that its redesigned website would monitor violent content using artificial intelligence and hide posts attacking individuals based on sex, sexual orientation, race, or religion using a trolling filter.[119] Currently, Parler is hosted by SkySilk Cloud Services, a seemingly libertarian web infrastructure company based in Los Angeles, California.[120] Before Amazon abruptly brought Parler offline, Parler claimed that it was valued at $1 billion.[121] Afterward, the company was worth substantially less.

Risk and Risk Assessments

One could argue that when assessing risk, the Parler example is an outlier, where the impact of the being taken offline was almost catastrophic, but the probability of occurrence was extremely low. When addressing risk, should one consider very high impact events with an extremely low probability of occurrence? If one uses the risk formula:

Risk Factor = Probability of Impact * Probability of Occurrence (2)

the risk factor result implies that such risks should be ignored or peripherally considered. For example, if the probability of impact is 0.99999 and the probability of occurrence is 0.00001, the risk factor becomes 0.00009, hardly a risk worth considering. However, according to Cooper et al., Eq. (1) is unacceptable because it ignores high impact probability and low occurrence probability risks.[122]

The corporate purchasing of cloud services is a large procurement, where millions of dollars are being spent on computing services. In contrast, Cooper et al. recommended that firms employ the following risk factor equation:[123]

Risk Factor = Probability of Impact + Probability of Occurrence –
(Probability of Impact * Probability of Occurrence) (3)

For example, suppose that the probability of impact is 0.99999 and the probability of occurrence is 0.00001. If Eq. (3) is used to calculate the risk factor, it becomes 0.99999, indicating the existence of a high risk that should and ought to be taken under serious consideration. On the other hand, if the probability of impact is 0.00001 and the probability of occurrence is 0.99999, when employing Eq. (3), the risk factor is also 0.99999. Although the risk factor in the second example is high, the fact remains that probability of impact is low. Thus, a risk with these values for the probability of impact and probability of occurrence can be safely ignored.

Cloud Computing versus On-Site Computing

Before the Parler debacle, many experts argued that cloud computing was an effective and low-cost computing solution.[124] After the Parler fiasco, times have changed. The issue facing billion-dollar firms is whether they are willing to bet the company by purchasing cloud computing services. If the cloud service provider suddenly decides that an entity has violated its terms of service, the cloud service provider, at its sole discretion, may decide to terminate service brusquely. Given that corporate data is the heart and soul of many Fortune 500 companies, the question facing these organizations is whether the termination of its ability to conduct business is worth the risk of putting its data on a cloud. For publicly traded companies and even private firms, the loss of business

---

[114] Ahiza García-Hodges, & Dennis Romero, *Parler Goes Offline After Amazon Hosting Suspension Over Violent Content*, NBC NEWS (Jan. 11, 2021) *available a*t https://www.nbcnews.com/tech/tech-news/amazon-suspends-hosting-parler-its-servers-citing-violent-content-n1253648.

[115] Bobby Allyn, *Judge Refuses To Reinstate Parler After Amazon Shut It Down*, NATIONAL PUBLIC RADIO (NPR) (Jan. 21, 2021), *available at* https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down.

[116] Rebecca Klar, *Parler Drops Federal Lawsuit Against Amazon, Files in State Court*, THE HILL (Mar. 3, 2021), *available at* https://thehill.com/policy/technology/541424-parler-drops-federal-lawsuit-against-amazon-files-in-state-court/.

[117] Kim Lyons, *Parler Resurfaces on Sunday with an Updated Timeframe*, THE VERGE (Jan. 17, 2021), *available at* https://www.theverge.com/2021/1/17/22236178/parler-resurfaces-sunday-app-banned.

[118] Ruth Bashinsky, *Parler Is Back Online With New Redesign and User Guidelines*, INSIDE EDITION (Feb. 18, 2021), *available at* https://www.insideedition.com/parler-is-back-online-with-new-redesign-and-user-guidelines-64973.

[119] Aaron Mak, *Parler Is Back and So Are Users Who Cheered on the Capitol Insurrection*, SLATE (Feb 18, 2021), *available at* https://slate.com/technology/2021/02/parler-capitol-riot-proud-boys-skysilk.html.

[120] Bobby Allyn, & Rachel Treisman, *After Weeks of Being Offline, Parler Finds a New Web Host*, NATIONAL PUBLIC RADIO (NPR) (Feb. 15, 2021), *available at* https://www.npr.org/2021/02/15/968116346/after-weeks-of-being-off-line-parler-finds-a-new-web-host.

[121] Grace Dean, *Parler Claims It Was Valued at $1 Billion Before Its Web Host Amazon Brought It Offline*, BUSINESS INSIDER (Mar. 3, 2021), *available at* https://www.businessinsider.com/parler-amazon-lawsuit-dropped-aws-antitrust-web-host-2021-3.

[122] DALE COOPER, STEPHEN GREY, GEOFFREY RAYMOND, & PHIL WALKER. PROJECT RISK MANAGEMENT GUIDELINES: MANAGING RISK IN LARGE PROJECT AND COMPLEX PROCUREMENT 67 (John Wiley & Sons 2003).

[123] *Id.*

[124] TechTarget, *supra*, note 95.

data may immediately translate into a sharp decline in its stock price and a deterioration of public confidence. According to *Dodge v. Ford*, the purpose of a corporation is to maximize shareholder value (i.e., its stock price).[125] Suppose the stock price of a company falls through the floor. In that case, stockholders will likely sue the company, the board of directors, and even senior management for a breach of fiduciary duty. The question facing organizations that store their data on a cloud is whether it is worth the risk. The risk occurrence depends on the company's business and what kinds of behavior and public statements it is willing to make.

Miscellaneous Considerations

Author Contributions: The author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Conflicts of Interest: The author declares no conflict of interest.
Acknowledgments: I acknowledge the insights on risk assessments and key risk indicators that I was fortunate enough to receive from Attorney Marc Roman. His comments were invaluable.

Abbreviations:

The following abbreviations are used in this manuscript:

Abbreviation	Description
Amazon	Amazon.com, Inc.
Apple	Apple Computer, Inc.
FBI	Federal Bureau of Investigation
IaaS	Infrastructure as a Service
KPI	Key Performance Indicator
KRI	Key Risk Indicator
NTCM	Nadler-Tushman Congruence Model
Parler	Parler Corporation
PaaS	Platform as a Service
SaaS	Software as a Service
SWOT	Strengths, Weaknesses, Opportunities, and Threats

CONCLUSION

According to *Citizens United*, corporations enjoy many free speech rights possessed by natural persons.[126] In the United States, commercial speech possesses substantial First Amendment protection, even though it is less than political, ideological, or artistic speech.[127] The ability of a cloud computing service provider to quell commercial speech should not be discounted. The Parler example reminds one that commercial speech is a right that companies should ardently seek to protect, not a right to be disregarded just because certain words have yet to be spoken. In deciding to embrace cloud computing, corporate eyes should be wide open, recognizing the risk of being cut off by a cloud computing provider, and be willing to experience the negative consequences if a catastrophic impact with an extremely low probability of occurrence manifests itself. Nothing less will suffice.

REFERENCES

1) Erin Doherty, & Oriana Gonzalez, In photos: An hour-by-hour record of the Jan. 6 Capitol riot, Axios (Jan. 6, 2022), available at https://www.axios.com/capitol-riot-january-6-anniversary-c61435e4-f4c4-4f5a-b6d1-9c463ac7eed2.html.
2) See generally, Thomas Dreisbach, Meg Anderson, & Barbara van Woerkom, 5 Takeaways from the Capitol Riot Criminal Cases, One Year Later, NATIONAL PUBLIC RADIO (Jan. 5, 2022), available at https://www.npr.org/2022/01/05/1070199411/5-takeaways-from-the-capitol-riot-criminal-cases-one-year-later.
3) Chris Cameron, These Are the People Who Died in Connection With the Capitol Riot, THE NEW YORK TIMES (Jan. 5, 2022), available at https://www.nytimes.com/2022/01/05/us/politics/jan-6-capitol-deaths.html.
4) Jack Nicas, &^ Davey Alba, Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters, THE NEW YORK TIMES (Jan. 9, 2021), available at https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html.

[125] *Dodge v. Ford*, *supra*, note 43.
[126] *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010).
[127] Alan B. Morrison, *How We Got the Commercial Speech Doctrine: An Originalist's Recollections*, 54 CASE WESTERN RESERVE L. REV. 4 (2004), *available at* https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1558&context=caselrev.

5) Intaver Staff, What are the benefits of project risk analysis?, INTAVER INSTITUTE (n.d.), available at https://intaver.com/blog-project-management-project-risk-analysis/benefits-project-risk-analysis/.
6) EPA Staff, Use of Monte Carlo Simulation in Risk Assessments: Use of Monte Carlo Simulation in Risk Assessments, UNITED STATES ENVIRONMENT PROTECTION AGENCY (n.d.), available at https://www.epa.gov/risk/use-monte-carlo-simulation-risk-assessments.
7) Lucid Content Team, A Complete Guide to the Risk Assessment Process, LUCIDCHART (n.d.), available at https://www.lucidchart.com/blog/risk-assessment-process.
8) Edafio Staff, 7 Crucial Questions To Ask During A Security Risk Assessment, EDAFIO TECHNOLOGY PARTNERS (n.d.), available at https://edafio.com/blog/7-crucial-questions-to-ask-during-a-security-risk-assessment/.
9) Jim DeLoach, 10 Questions You Should Ask About Risk Management, CORPORATE COMPLIANCE INSIGHTS (Feb. 18, 2018), available at https://www.corporatecomplianceinsights.com/ten-questions-you-should-ask-about-risk-management/.
10) Will Kenton, Gordon Scott, & Ariel Courage, Strength, Weakness, Opportunity, and Threat (SWOT) Analysis, INVESTOPEDIA (Updated Mar. 29, 2021), available at https://www.investopedia.com/terms/s/swot.asp.
11) CHARLES W. L. HILL, & GARETH R. JONES, STRATEGIC MANAGEMENT: AN INTEGRATED APPROACH 5 (Houghton Mifflin Company 1998).
12) Sling Staff, Functional Level Strategy: What It Is Plus 18 Examples, SLING (n.d.), available at https://getsling.com/blog/functional-level-strategy/.
13) Richard Lynch, Global Strategy – Definition and Meaning, MARKET BUSINESS NEWS (n.d.), available at https://marketbusinessnews.com/financial-glossary/global-strategy/.
14) Sling Staff, supra, note 27 .
15) Brian Willis, Three Categories of Security Controls, LMBC FAMILY OF COMPANIES (n.d.), available at https://www.lbmc.com/blog/three-categories-of-security-controls/.
16) Charles W. L. Hill, & Gareth R. Jones, supra, note 23 at 144.
17) MICHAEL E. PORTER, COMPETITIVE ADVANTAGE: CREATING AND SUSTAINING SUPERIOR PERFORMANCE (The Free Press 1985).
18) Dodge v. Ford Motor Company, 204 Mich. 459, 170 N.W. 668 (Mich. 1919) (here, the court opined that the purpose of a company is to maximize shareholder value).
19) Jason Fernando, Thomas Block, & Pete Rathburn, Stakeholder, INVESTOPEDIA (Aug. 19, 2021), available at https://www.investopedia.com/terms/s/stakeholder.asp.
20) Katie Terrell Hanna, & Francesca Sales, Gap Analysis, TECHTARGET (Oct. 2021), available at https://www.techtarget.com/searchcio/definition/gap-analysis.
21) Charles W. L. Hill, & Gareth R. Jones, supra, note 23.
22) Katie Terrell Hanna, & Francesca Sales, supra, note 45.
23) Charles W. L. Hill, & Gareth R. Jones, supra, note 23.
24) Katie Terrell Hanna, & Francesca Sales, supra, note 45.
25) Mind Tools Content Team, McKinsey 7-S Framework: Making Every Part of Your Organization Work in Harmony, MIND TOOLS (n.d.), available at https://www.mindtools.com/pages/article/newSTR_91.htm.
26) Performance, MIND TOOLS (n.d.), available at https://www.mindtools.com/pages/article/newSTR_95.htm.
27) Mind Tools Content Team, supra, note 54.
28) Mind Tools Content Team, supra, note 60.
29) TechTarget Staff, Key Risk Indicator (KRI), TECHTARGET (Oct. 2021), available at https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI.
30) SolveXia Staff, Key Risk Indicators: Examples and Definitions, SOLVEXIA (Dec. 15, 2020), available at https://www.solvexia.com/blog/key-risk-indicators.
31) TechTarget Staff, supra, note 71.
32) GLYN A. HOLTON, VALUE AT RISK: THEORY AND PRACTICE (Academic Press 2003).
33) Jake Frankenfield, & Julia Mansa, Cloud Computing, INVESTOPEDIA (Jul. 28, 2020), available at https://www.investopedia.com/terms/c/cloud-computing.asp.
34) TechTarget Staff, Cloud Computing, TECHTARGET (Dec. 2021), available at https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.
35) Alexis Benveniste, & Kaya Yurieff, Meet Rebekah Mercer, the Deep-Pocketed Co-Founder of Parler, a Controversial Conservative Social Network, CABLE NEWS NETWORK (CNN) (Nov. 16, 2020), available at https://www.cnn.com/2020/11/15/media/rebekah-mercer-parler/index.html.

36) Mark Di Stefano, Alex Spence, & Ryan Mac, Pro-Trump Activists Are Boosting a Twitter App Used by Banned Personalities and It Appears to Have Already Stalled, BUZZFEED NEWS (Feb. 12, 2019), available at https://www.buzzfeed.com/markdistefano/pro-trump-activists-are-boosting-a-twitter-app-for-banned.
37) Isaac Saul, This Twitter Alternative Was Supposed to Be Nicer, but Bigots Love It Already, FORWARD: JEWISH, INDEPENDENT, NON-PROFIT (Jul. 18, 2019), available at https://forward.com/news/427705/parler-news-white-supremacist-islamophobia-laura-loomer/.
38) Brian C. Parker, I Tried Parler, the Social Media App Where Hate Speech Thrives, CHRON ()Dec. 01, 2020), available at https://www.chron.com/news/article/I-tried-Parler-the-social-media-app-where-hate-15765465.php.
39) Keach Hagey, & Jeff Horwitz, Parler, a Platform Favored by Trump Fans, Struggles for Survival, THE WALL STREET JOURNAL (Jan. 11, 2021), available at https://www.wsj.com/articles/parler-struggles-survival-amazon-lawsuit-trump-fans-11610414745.
40) Craig Timberg, & Drew Harwell, Pro-Trump Forums Erupt with Violent Threats Ahead of Wednesday's Rally Against the 2020 Election, THE WASHINGTON POST (Jan. 5, 2021), available at https://www.washingtonpost.com/technology/2021/01/05/parler-telegram-violence-dc-protests/.
41) Sheera Frenkel, The Storming of Capitol Hill Was Organized on Social Media, THE NEW YORK TIMES (Jan. 6, 2021), available at https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html.
42) Aaron C. Davis, Red Flags, THE WASHINGTON POST (Oct. 31, 2021), available at https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/.
43) Betsy Woodruff Swan, & Nicholas Wu, Secret Service Warned Capitol Police About Violent Threats 1 Day before Jan. 6, POLITICO (Aug. 25, 2021), available at https://www.politico.com/news/2021/08/25/secret-service-warned-capitol-police-violent-threats-january-riot-506806.
44) Aleszu Bajak, Jessica Guynn, & Mitchell Thorson, When Trump Started His Speech Before the Capitol Riot, Talk on Parler Turned to Civil War, USA TODAY (Feb. 1, 2021), available at https://www.usatoday.com/in-depth/news/2021/02/01/civil-war-during-trumps-pre-riot-speech-parler-talk-grew-darker/4297165001/.
45) John Paczkowski, & Ryan Mac, Amazon Will Suspend Hosting for Pro-Trump Social Network Parler, BUZZFEED NEWS (Jan. 9, 2021), available at https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws.
46) Ashley Gold, & Shawna Chen, Google Suspends Parler from App Store After Deadly Capitol Violence, AXIOS (Jan. 8, 2021), available at https://www.axios.com/capitol-mob-parler-google-ban-826d808d-3e06-4468-a7c6-6157557818b3.html.
47) Emma Bowman, Amazon and Apple Drop Parler, NATIONAL PUBLIC RADIO (NPR), (Jan. 9, 2021), available at https://www.npr.org/2021/01/09/955329265/amazon-and-apple-drop-parler.
48) Annie Palmer, Amazon Drops Parler from Its Web Hosting Service, Citing Violent Posts, CNBC (Jan. 9, 2021), available at https://www.cnbc.com/2021/01/09/amazon-drops-parler-from-its-web-hosting-service.html.
49) Ahiza García-Hodges, & Dennis Romero, Parler Goes Offline After Amazon Hosting Suspension Over Violent Content, NBC NEWS (Jan. 11, 2021) available at https://www.nbcnews.com/tech/tech-news/amazon-suspends-hosting-parler-its-servers-citing-violent-content-n1253648.
50) Bobby Allyn, Judge Refuses To Reinstate Parler After Amazon Shut It Down, NATIONAL PUBLIC RADIO (NPR) (Jan. 21, 2021), available at https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down.
51) Rebecca Klar, Parler Drops Federal Lawsuit Against Amazon, Files in State Court, THE HILL (Mar. 3, 2021), available at https://thehill.com/policy/technology/541424-parler-drops-federal-lawsuit-against-amazon-files-in-state-court/.
52) Kim Lyons, Parler Resurfaces on Sunday with an Updated Timeframe, THE VERGE (Jan. 17, 2021), available at https://www.theverge.com/2021/1/17/22236178/parler-resurfaces-sunday-app-banned.
53) Ruth Bashinsky, Parler Is Back Online With New Redesign and User Guidelines, INSIDE EDITION (Feb. 18, 2021), available at https://www.insideedition.com/parler-is-back-online-with-new-redesign-and-user-guidelines-64973.
54) Aaron Mak, Parler Is Back and So Are Users Who Cheered on the Capitol Insurrection, SLATE (Feb 18, 2021), available at https://slate.com/technology/2021/02/parler-capitol-riot-proud-boys-skysilk.html.
55) Bobby Allyn, & Rachel Treisman, After Weeks of Being Offline, Parler Finds a New Web Host, NATIONAL PUBLIC RADIO (NPR) (Feb. 15, 2021), available at https://www.npr.org/2021/02/15/968116346/after-weeks-of-being-off-line-parler-finds-a-new-web-host.
56) Grace Dean, Parler Claims It Was Valued at $1 Billion Before Its Web Host Amazon Brought It Offline, BUSINESS INSIDER (Mar. 3, 2021), available at https://www.businessinsider.com/parler-amazon-lawsuit-dropped-aws-antitrust-web-host-2021-3.

57) DALE COOPER, STEPHEN GREY, GEOFFREY RAYMOND, & PHIL WALKER. PROJECT RISK MANAGEMENT GUIDELINES: MANAGING RISK IN LARGE PROJECT AND COMPLEX PROCUREMENT 67 (John Wiley & Sons 2003).
58) TechTarget, supra, note 95.
59) Dodge v. Ford, supra, note 43.
60) Citizens United v. Federal Election Commission, 558 U.S. 310 (2010).
61) Alan B. Morrison, How We Got the Commercial Speech Doctrine: An Originalist's Recollections, 54 CASE WESTERN RESERVE L. REV. 4 (2004), available at https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1558&context=caselrev.