Journal of Business, Accounting and Finance Perspectives

Digital Liability Risk: A Note on Estimating Exposure, Costs, and Implications

Robyn L. Raschke [1,*], Michael T. Lee [2], Kimberly F. Charron [1], Paulette R. Tandy [1]

[1] Lee Business School, Accounting Department, University of Nevada, Las Vegas, NV 89154, USA
[2] SKEMA Business School, 920 Main Campus Drive, Raleigh, NC 27606, USA; michael.lee@skema.edu
* Corresponding author: robyn.raschke@unlv.edu

Submitted: 27 August 2019, accepted: 8 January 2020, published: 10 February 2020

Abstract: Digital liabilities are the unknown future costs that occur after an event related to digital assets threatens organizational value. These events emerge from: (1) an IT data breach or cybersecurity failure; (2) IT infrastructure limitations that limit future opportunities; and (3) changes in business models that are limited due to IT infrastructure. Potential digital liabilities are not fully understood and can be difficult to quantify. Derived from prior research, this research note proposes four methods, modified from existing research literature, for estimating the cost of digital liabilities prior to a digital asset compromise. We conclude the research note by discussing opportunities for future research in this area.

Keywords: digital assets; digital liability; risk; valuation

How to cite: Robyn L. Raschke, Michael T. Lee, Kimberly F. Charron, Paulette R. Tandy.Digital Liability Risk: A Note on Estimating Exposure, Costs, and Implications. *J. Bus. Account. Financ. Perspect.*, 2020, 2(1): 1; doi:10.35995/jbafp2010001.

1. Introduction

The balance sheet is a statement of what a company owns (assets), owes (liabilities), and the amount invested by its owners (shareholder equity). Consequently, the balance sheet demonstrates the financial position of a company (Harrison et al., 2017). However, current investor valuation trends show that companies with digital assets are generally valued higher than equivalent companies with physical assets[1]. For example, Amazon, an online retailer with distribution centers and no physical stores, is valued greater than brick-and-mortar Walmart, Costco, and

[1] https://www.nytimes.com/2016/08/28/technology/ge-the-124-year-old-software-start-up.html?_r=0.

Target[2]. Airbnb, a market aggregator of vacation rental accommodation with no physical vacation properties, is valued greater than many hotel chains such as Hilton, Hyatt or Marriott[3].

Although there are three overall approaches to business valuation, (1) market-based approaches, (2) asset-based approaches, and (3) income approaches, the current trend suggests that market-based approaches are taking precedence over asset-based approaches (see Cohen, 2011). The intangible value of digital assets appears to be incorporated into stock prices, explaining some of the difference in the valuation of digital versus physical companies.

Another aspect to consider is that a complete valuation of the financial position of a company also requires an accurate assessment of the potential liabilities associated with possessing digital assets. Plunging stock prices after digital assets are compromised provide evidence that stock valuations do not fully incorporate the potential liabilities associated with digital assets. In general, financial reporting generally accepted accounting principles (GAAP) focus on reporting obligatory liabilities, and a liability may not be acknowledged and recorded until after an event that compromises digital assets occurs. In 2017, a multitude of security failures resulted in data breaches and significant losses in value for the affected companies. The most well-known failure was Equifax, where 143 million consumers had sensitive personal information stolen. Hackers gained access to the company's system from mid-May to July by exploiting a weak point in website software[4]. After the data breach was announced to the market on 7 September 2017, the Equifax share price dropped approximately 35% in the first week[5]. Security failures have had similar effects at companies such as Whole Foods Market, Verizon, and Sonic[6]. Like the tips of an iceberg, the potential costs associated with these valuable digital assets lie beneath the balance sheet waterline and remain unseen until those digital assets are compromised. Even the initial stock market impact is not the full story. Related costs are often incurred for years after an incident due to externalities created, such as damaged reputation, lawsuits, lost supplier relationships or regulatory enforcement actions[7].

Digital liabilities, while difficult to quantify, have important implications for company management. Management must determine potential risks at the organizational level and identify the need to mitigate significant threats to digital assets. This research note has three objectives: (1) to provide a definition of potential digital liabilities as they relate to digital assets; (2) to propose methods for estimating the likely exposure to digital liabilities; and (3) to discuss the implications of digital liabilities for practice as well as future research opportunities.

This research note is structured as follows. Section 2 presents a discussion on the nature of digital liabilities and provides a suitable definition. Sections 3 and 4 propose methods for estimating the costs associated with digital liabilities and consider the advantages and disadvantages of the methods. Section 5 discusses the implications of digital liabilities for internal stakeholders in management and risk mitigation as well as external stakeholders. This discussion also outlines opportunities for future research.

2. Organizational Digital Liabilities

Digital liabilities are the unknown future costs that occur after an event related to digital assets threatens organizational value. Potential digital liabilities are not fully understood and can be difficult to value because they are difficult to identify and quantify. Despite not being fully comprehended, these risks are on the radar screen of many companies. According to a recent survey by Protiviti and North Carolina State University's ERM Initiative, corporate board members considered cyber threats and privacy/identity management and information security as two of the top five areas of concern for 2017[8]. Any event that compromises the value of digital assets gives rise

[2] http://fortune.com/2017/04/05/amazon-walmart-costco-target-market-cap/.
[3] https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/briansolomon/2016/09/22/airbnb-fundraising-850-million-30-billion-valuation/&refURL=https://www.google.com/&referrer=https://www.google.com/.
[4] https://www.washingtonpost.com/news/the-switch/wp/2017/09/20/the-single-most-depressing-thing-about-the-equifax-breach/?utm_term=.de8c1941d43d.
[5] https://finance.yahoo.com/quote/EFX.history?p=EFX.
[6] https://www.identityforce.com/blog/2017-data-breaches.
[7] https://blog.centrify.com/breaches-negative-impact-brand-reputation/.
[8] http://bit.ly/2hdeqNQ.

to digital liabilities. These events, explained below, usually emerge from: (1) an IT data breach or cybersecurity failure; (2) IT infrastructure limitations that limit future opportunities; and/or (3) changes in business models that are limited due to IT infrastructure.

Digital liabilities most commonly arise from cybersecurity failure in the form of data breaches due to hacking, ransomware, and denial-of-service attacks[9]. Research has shown that hackers are able to remotely hijack drones, industrial control systems, automobiles, traffic lights, and essentially anything connected to the internet or digitally powered (Rohrer and Hom, 2017). This opens up an infinite number of possible areas of exposure for most firms. Ransomware is also a cybersecurity threat to companies. Ransomware allows hackers to encrypt data, rendering data inaccessible or "locked" throughout a network until a ransom is paid. Similarly, in denial-of-service (DDoS) attacks, hackers make a network resource unavailable either temporarily or indefinitely. DDoS attacks can cost companies up to $40,000 per hour as their website goes offline[10]. The 2016 attack against Dyn, one of a handful of "domain name server (DNS)" providers, brought down all web addresses registered with its service, such as Merck[11], Twitter, Reddit, eBay, The Telegraph, and many more.

Digital liabilities also arise from limitations to IT infrastructure and pose a risk to an organization's strategy. For example, missed opportunities can occur when an organization's IT infrastructure is outdated, and a merger or acquisition becomes more difficult to support. An organization's IT platform, applications, and business processes require consideration during the due diligence of a merger or acquisition (Khazanchi and Arora, 2016). The lack of IT infrastructure to support the organization is detrimental to the post-merger/acquisition success of the company. If the combined business is unable to process data in an efficient manner with due regard to security, there is potential for business interruption, loss of data, and inaccurate or unauthorized changes to data that ultimately can lead to a loss of data integrity or fraud (Tarasovich et al., 2008). For example, a merger delay was announced by two pharmaceutical companies due to incompatible IT infrastructure[12]. In an example from the airline industry, the merger of America West and US Airways in 2005 illustrates the importance of IT. The combined company experienced significant difficulties when the reservation and ticketing programs were integrated and the new system could not communicate with airport kiosks, resulting in days of missed flights, delays, and angry customers. IT problems can also arise when integrating flight tracking systems, customer information data for rewards programs and upgrades, and other important systems. In the Continental–United merger, millions were spent to navigate the integration (Credeur, 2012).

Furthermore, the business landscape is a changing environment, and organizations change their business models to remain competitive in the marketplace. The ability to change your business model requires a flexible IT infrastructure and agility (Sambamurthy et al., 2003; Raschke, 2010). Organizations must adopt new business models to stay relevant and successful in a rapidly-changing economic environment. Changing business models with old and outdated IT platforms exposes these companies to events that may be very likely to compromise their digital assets (Wessel et al., 2015).

In summary, digital liabilities are the unknown future costs that occur after an event compromises the value of digital assets. Digital liabilities can arise with cybersecurity failures, missed opportunities and changes in business models due to IT limitations. While the risk of digital liabilities may be easily identified, quantifying the impact of digital liabilities may be difficult for management.

3. Estimating the Cost of Potential Digital Liabilities

There are several types of costs that are associated with digital liabilities. Some are preventative costs, such as antispyware software and backup systems, which are measurable and reflected in the accounting records.

[9] https://www.identityforce.com/blog/data-breach-statistics-2016-vs-2015.
[10] http://www.telegraph.co.uk/technology/0/what-is-a-ddos-attack-and-could-my-computer-be-a-weapon/.
[11] https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO.
[12] http://www.independent.co.uk/news/business/news/glaxo-facing-staff-exodus-as-delays-to-merger-hit-morale-635591.html.

Other measurable costs are incurred after a digital asset is compromised, such as customer compensation, legal fees or fines, and are recorded in the financial records after the compromise. However, hidden costs, such as damaged brand credibility and general reputation, loss of future revenue and market share, and the potential costs related to future regulations or oversight are rarely, if ever, recorded. From an internal strategic management perspective, managers need to understand digital liability risk from digital assets regardless of financial statement reporting requirements. This research note proposes four methods, modified from existing research literature, for estimating the complete cost of digital liabilities prior to a digital asset compromise.

3.1. The Multiplier Method

The multiplier method states that the total digital liability (TL) is a multiple of the measured costs of digital liabilities (MC), which include preventative costs and the actual costs incurred after a compromise:

$$\mathrm{TL} = k \times \mathrm{MC},$$

where TL = Total liability, k = the multiplier, and MC = measured digital liability cost.

The value of k is based on past experience of a multiple of the MC (measured digital liability costs). Formal market research methods are used to quantify the effect of cybersecurity failure, IT infrastructure limitations, and/or failure of digital assets on a company's brand credibility and general reputation by examining expected future sales and market share. Customer surveys, focus groups, and interviews with members of a company's salesforce can provide significant insights into the magnitude of a company's digital liability exposure and the likely hidden costs that come from lower expected future sales and market share.

3.2. The Taguchi Loss Function

The Taguchi loss function (Deming, 1993) is an advanced version of the multiplier method that can potentially capture the hidden costs of compromises in digital assets. The premise of this concept/function is that poor product *quality* costs more than simply replacing a product or providing warranty work. In the longer term, the product may possibly wear out sooner, need to be replaced, cause defects in other interrelated products, and ultimately lead to hidden costs such as those related to customer defection and damaged reputation. This same concept/function can be applied to estimating total digital liabilities. As Baker et al. (2017) stated, there are both compliance and noncompliance costs with keeping data. Compliance costs would include but are not limited to purchasing antispyware programs, installing patches/upgrades to systems, and audits of data security measures. The noncompliance costs would include but are not limited to cyberattack cleanups, legal defense costs, fines, settlement costs, as well as damage to reputation and loss of customers or value chain partners. The function assumes that any variation from a target value of a quality characteristic (compliance costs) causes longer-term costs that are not immediately quantified (noncompliance costs).

The Taguchi loss function is a quadratic equation:

$$\mathrm{TL}\ (\mathrm{y}) = k\ (\mathrm{y} - \mathrm{T})^2.$$

In the context of software upgrades, TL (y) = the total potential liability cost associated with a software failure, k = the multiplier effect, y = the actual cost of safeguarding digital assets (in this context, the actual expenditures on software upgrades), and T = the target cost of safeguarding digital assets (in this context, the expenditures on software upgrades). To apply the Taguchi loss function, k must be estimated. The value of k is computed by dividing the estimated cost at one of the specification limits by the squared deviation of the limit from the target value, or $k = \mathrm{c}/\mathrm{d}^2$, where k = the multiplier effect, c = the estimated cost at one of the specification limits, and d = the deviation of the limit from the target value. Applying this method, an estimate of the liability for a given deviation from the target value is still needed. Sampling and surveying customers and market research are used to make this estimation.

To provide another illustration of how this function is used, consider the common example of a cybersecurity failure involving a retail ecommerce company with a digital customer list containing personal details[13]. This customer list is critical, as it allows the company to generate revenue from customers' online purchases by authenticating customer personal details. The retail ecommerce company typically uses customer information retrieval response time as a measure of customer experience quality. Since the Taguchi function is a quadratic function, reducing security may improve customer information retrieval response time, but this will increase the hidden liability costs at an *exponentially increasing rate*. Conversely, increasing security will slow customer information retrieval response time because of the many layers of encryption[14], and slow response times are a known cause of customer abandoned shopping carts. Consequently, liability costs also *increase exponentially* if the company spends more than its target cost for safeguarding digital assets.

3.3. Probabilistic Models

The methods for estimating digital liabilities above rely on the establishment of a multiplier, which is not always easy to achieve. Probabilistic models (Koller, 2005; Amit and Wernerfelt, 1990) can also be used to estimate digital liabilities. Probabilistic models combine probabilities of each cybersecurity failure, IT limitation, and/or failure of digital assets with the respective loss due to compromised digital assets to determine an expected value of the associated risk. This is known as the risk exposure (RE) and in a basic form is measured as follows:

$$\mathrm{RE} = \mathrm{P(uo)} \times \mathrm{L(uo)},$$

where RE = the cost of risk exposure, P(uo) = the probability of a cybersecurity failure, IT limitation, and/or failure of digital assets, and L(uo) = the loss due to a cybersecurity failure, IT limitation, and/or failure of digital assets.

The total digital liability is calculated by assessing the sum of the expected REs. Applying probabilistic models involves estimating all of the possible losses due to compromised digital assets and the probabilities of these losses occurring. These estimates are difficult to quantify because a compromise of digital assets can occur at any time, and the effect can vary greatly. Therefore, an incorrect assessment of RE may result in a less than useful value of the company's digital liabilities. To improve the probability estimates, fuzzy neural networks and artificial neural networks can be employed. These are discussed in detail below.

3.4. Event Studies

An event study (Fama et al., 1969) is a powerful method that helps researchers to assess the financial impact of changes in corporate activities. As it is considered a market-based approach to business valuation, researchers use this method to determine whether there is an *abnormal* stock price effect associated with an unanticipated event. Abnormal stock price changes can infer the effect of the event on the value of the company. This method is frequently used in accounting and finance to measure the impact of corporate control changes (Sorescu et al., 2017). In management, the method is used to judge the effects of endogenous corporate events, such as corporate refocusing, CEO turnover, layoffs, plant closures, corporate illegalities, product recalls, customer service changes, and strategic investment decisions (Oler et al., 2008; Binder, 1998; McWilliams and Siegel, 1997). Therefore, this approach can also apply to calculating the effects of unanticipated compromises of digital assets on company value.

Event studies are popular because stock prices are used to reflect the value of companies rather than accounting profits, which can be subject to manipulation and may not always adequately reflect a company's future value (Sorescu et al., 2017). Stock prices are assumed to reflect the discounted value of all future cash flows and incorporate all relevant information. Therefore, event studies, which are based on stock price changes, should measure the financial impact of any change in corporate activities. Furthermore, the event study method is relatively easy to implement because the only data necessary are the names of publicly traded companies, event dates, and stock prices.

[13] https://www.identityforce.com/blog/data-breach-statistics-2016-vs-2015.
[14] http://www.webperformancetoday.com/2012/08/14/page-speed-vs-security/..

In sum, event studies can be used to calculate digital liabilities because researchers can measure the abnormal returns from stock prices from the announcement of compromised digital assets. For example, the digital liabilities from the cybersecurity failures at Equifax, Verizon, and FedEx can be calculated from the negative abnormal decreases in the stock prices when these publicly-listed companies made their data breach announcements.

4. Choosing a Method

Because digital liabilities are difficult to estimate and there are several approaches organizations can apply, companies will generally choose an estimation method based on the information that is available to them. However, multiple methods are recommended to ensure confidence in the estimate. The various methods for estimating digital liabilities may have advantages and disadvantages in their applications. Table ?? summarizes the advantages and disadvantages of the methods.

	Advantages	Disadvantages
Multiplier Method	Simple to apply, simple to use	Difficult to estimate multiplier, ignores the likelihood and hidden consequences of a compromise
Probability Models	Identifies factors leading to compromises and probabilities of compromises, applies probabilities to various measurable liabilities, can be extended using fuzzy logic and artificial neural networks	Difficult to estimate probabilities and hidden costs
Event Studies	Market-based approach to estimating digital liabilities, uses publicly available information	Only possible for publicly-traded companies, methodological assumptions may limit its meaningfulness

Table 1 Comparing methods for estimating digital liabilities.

In this section, the various approaches are discussed in to the context of an attack on point-of-sale (POS) systems or cash register systems, the most common form of cybersecurity failure[15]. Many retail companies may be slow to install software patches, even for known security problems, because they fear the patches might disable their POS systems and cause them to lose sales. The inconvenience is compounded by the increased frequency of the recommended security updates, in response to known or potential security breaches.

In attacks on POS systems, hackers insert malicious software into a company's system. The malware surreptitiously records credit and debit card information when customers swipe their cards through the payment terminals. The card information is sent to the hackers, who sell it on the internet underground or dark web. These breaches can lead to significant losses for retailers and their customers. For example, Target agreed to pay $18.5 million to resolve investigations into the attack that affected more than 41 million of the company's customer payment card accounts in 2013[16]. To date, each stolen record has been estimated to cost retailers an average of $141[17].

4.1. Applying a Multiplier

Applying the simple multiplier model provides a quick method for determining digital liabilities. In the POS system example, the multiplier is $141 for each customer record according to an IBM survey[18]. Therefore, the potential

[15] https://www.identityforce.com/blog/data-breach-statistics-2016-vs-2015.
[16] http://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/.
[17] https://www.ibm.com/security/data-breach/index.html.
[18] https://www.ibm.com/security/data-breach/index.html.

digital liability is 141 times the number of customer records held by the retail company. Once a multiplier is estimated, organizations can conduct sensitivity analyses regarding the potential digital liability by varying the multiplier to calculate a range of estimates from conservative to optimistic. While this method is based on existing customers, the companies could forecast the future potential digital liabilities by including a calculation for the anticipated growth in the company's customer base. However, in reality, the multiplier k is generally difficult to estimate. Historic values from previous events within an industry may not be applicable to all firms or situations. Having timely data based on current threats and fall-out costs requires constant review of the digital landscape.

Another key limitation of using the simple multiplier method is the omission of two important dimensions of the total potential digital liability, the likelihood of a cybersecurity failure, and the hidden consequences of the failure (although the Taguchi loss function attempts to capture these externalities). A company can estimate and understand the financial impact of a cybersecurity failure using a multiplier, but that result does not communicate the probability of the cybersecurity failure occurring. A failure may cost a company millions of dollars, but what is the probability that a specific failure would occur? Is it going to be five percent, ten percent or more? At the same time, the multiplier does not incorporate any nonfinancial consequences of the cybersecurity failure. Even if the multiplier is small and/or the probability of a failure is small, the consequences of compromising customer data privacy could fatally damage a company's reputation.

4.2. Using Probability Models

Traditional probability models overcome a limitation of applying a multiplier by incorporating the probability of a cybersecurity failure with the expected measurable loss from the failure. Assessing probabilities requires the identification of the factors that cause cybersecurity failures (e.g., Angst et al., 2017) and an evaluation of the significance of these factors in a company's environment. Applying the context of a POS security breach, a company would apply a probability model by estimating both the projected loss from a breach and the probability of a breach occurring (based upon the current internal controls protecting the POS system data).

In determining the expected loss, probability models incorporate the financial consequences of cybersecurity failures (e.g., the hardware and software required to repair and secure private information and the cost of compensating clients and customers) but may not account for the hidden consequences of these events. The damage to a company's brand credibility and general reputation may not be easily understood or quantified.

Because there are inherent difficulties in determining probabilities, we suggest that fuzzy logic and artificial neural networks may help to improve the accuracy of estimating digital liabilities by reducing human bias or error associated with the weighting and combining of risk factors and their related costs (see Siddique and Adeli (2013)). Fuzzy logic and artificial neural network software can be purchased and embedded within any computing hardware, including mobile phones, and recognize a range of possible outcomes by assigning cumulative probabilities to the entire range of possible digital liabilities (Lin et al., 2003). The power of this approach is the ability to handle multiple decision rules simultaneously where there are subtle gray areas (Lin et al., 2003). Neural networks can use a list of pertinent factors and their consequences in combination with traditional probability models to calculate digital liabilities.

Because risk probability is difficult to assess, an integrated system of fuzzy logic and neural networks can be used to provide a scientific method for assessing probably liabilities from cybersecurity failure. Prior research in accounting, specifically Eining et al. (1997), Piramuthu (1999) and Coderre (2000), find that a logit model achieves more accurate risk assessment than either a checklist of risks or unaided decision makers. These decision support tools can help to improve the accuracy of estimating digital liabilities by reducing human bias or error associated with the weighting and combining of risk factors.

Fuzzy logic is a logical system used to operate on fuzzy sets. First proposed by Zadeh (1965), fuzzy logic has gained popularity with applications found in areas ranging from consumer products marketing to industrial process control and portfolio management (Cox, 1992; Trippi and Turban, 1996). Fuzzy logic is applied in research on

investment (Tanaka et al., 1976), project cost estimation (Turunen et al., 1984), business planning (Hruschka, 1988), financial ratio analysis (Gutierrez and Carmona, 1988), commercial loan analysis (Levy et al., 1991), stock selection (Wong et al., 1992), and temperature control systems (Port and Raeburn, 1999).

Information available for decision making is not usually black or white but generally involves some subtle gray areas. Fuzzy sets and fuzzy logic are developed to represent, manipulate, and utilize uncertain information and to provide a framework for handling uncertainty and imprecision in real-world applications. Fuzzy logic systems accomplish this by allowing a computer to simulate human reasoning with less bias and to behave with less analytical decision and logic than conventional computing methods (Turban and Aronson, 2000). Fuzzy logic systems recognize this range of possibilities by assigning cumulative probabilities to the entire range of possible outcomes. The power of this approach becomes apparent when multiple decision rules are simultaneously applied.

Artificial neural networks are computer programs that simulate the way the human brain functions. The basic building blocks of human brains are neurons, which process numerous inputs to produce outputs. These artificial neural networks consist of simulated neurons in the format of layers and nodes. They have an ability to learn through trial and error where neurons adjust their weights of input variables to model the behavior or patterns of output levels. These networks have been employed to solve a variety of financial problems, including bank failure prediction (Tam and Kiang, 1992), stock picking (Kryzanowski et al., 1993), option pricing (Barucci et al., 1996), and management fraud detection (Eining et al., 1997).

In summary, solutions from fuzzy logic and neural networks are generally more robust, flexible, and economical than those provided by traditional probabilistic models. Furthermore, fuzzy logic and neural networks are complementary rather than competitive to traditional probabilistic models.

4.3. Conducting an Event Study

Event studies are used when a company is listed on a stock exchange, and trading in the company stock is liquid. With private companies, however, event studies cannot be conducted because relevant pricing and financial information is not publicly available. Therefore, the application of this method of estimating digital liability from cybersecurity failure is limited to publicly held organizations.

Assuming that an event study can be conducted, there are other well-known limitations to consider (Sorescu et al., 2017). First, event studies assume that the market is efficient. Market efficiency implies that stock prices incorporate all relevant information available to market traders. Therefore, any financially relevant information that is newly revealed to investors will be quickly and instantaneously incorporated into stock prices. A cybersecurity failure results in new relevant information, and a researcher can identify the impact on stock prices of a company by defining a period of days over which the impact of the compromising event will be measured. However, market efficiency is difficult to reconcile with the use of a long event window, and determining the appropriate event window may be challenging.

Second, the model assumes that the market did not previously have information concerning the cybersecurity failures before the failures are announced in the press. Abnormal positive or negative returns are expected to be a result of the stock market reacting to the new information. If the cybersecurity failure is already known prior to the press announcement, some of the market reaction to the information is diluted.

Third, there may also be confounding effects from other events. Isolating the effect of a cybersecurity failure from the effects of other events may be difficult or impossible. Confounding events could include but are not limited to an announcement of a new product, a merger, an acquisition, the filing of a large damage suit or a change in a key executive. Fourth, the sample size of cybersecurity failures in companies is still relatively small, and each cybersecurity failure is different. Additional information is needed to predict the effect of a cybersecurity failure on companies.

5. Implications for Stakeholders and Future Research

Digital liabilities impact both internal and external stakeholders. From an internal stakeholder perspective, organizational management needs to understand the potential risks and estimate the potential value impact of digital liabilities. Understanding the magnitude of potential digital liabilities allows management the opportunity to take action to mitigate the risk or share the risk by adequately insuring against such losses. The market for insuring companies against cybersecurity breaches is growing, and most policies are currently based on self-assessment (Reber, 2017). Having a better understanding of the probabilities and magnitude of potential costs can reduce later out-of-pocket expenses.

Management is best suited from an enterprise risk management perspective to be proactive and manage these risks within the tolerance of their risk appetite. Since risk management focuses on identifying and assessing risk that impedes an organization from achieving their strategic goals and objectives, leveraging strategic management research within the context of digital liabilities provides additional insights. For example, further research is needed to help to understand the role of top management support as well as the organization's culture relative to the digital liabilities context.

External stakeholders such as investors and policy makers are also impacted by digital liabilities. As more companies fall victim to failures related to digital assets, policy makers need to consider whether information concerning digital liabilities may need to be presented. Would information provided in a footnote or narrative description in the annual report be sufficient or would formal recognition of an estimated digital liability within the balance sheet be warranted? Researchers should explore the information content of different options to investors and other stakeholders. Researchers should also investigate the potential effect on decision making resulting from different presentations of digital liabilities,

In addition, more research is needed concerning assurance as it relates to IT security and infrastructure limitations. Pursuant with the Sarbanes–Oxley Act, audits currently provide assurance regarding internal controls, including IT security controls. However, do these assurance processes adequately address the potential liabilities from compromised digital assets? If not, who should provide this assurance? Should the responsibility be assumed by the organization's financial statement auditors or would a specialized assurance process be warranted?

Different stakeholder information requirements may be appropriate when addressing digital liabilities that result from cyberattacks vs. IT infrastructure. The reporting requirements of companies may even vary based on different types of cyberattacks (i.e., those like ransomware or DDoS attacks or theft of customer information). Exploring how each type of digital liability impacts the various stakeholders (both internal and external) would also be informative for risk management and strategic decision making. More research is needed in examining the efficacy of each method or the use of multiple methods on company valuations.

In conclusion, this research note has defined and described digital liability risk and the importance of understanding these risks for management purposes. In addition, several methods are discussed to estimate the risk exposure of digital liability risks as well as areas for future research.

References

Amit, R., & Wernerfelt, B. (1990). Why do firms reduce business risk? *Academy of Management Journal*, *33*(3), 520–533. [CrossRef]

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893–916. [CrossRef]

Baker, W. M., Kemerer, K. L., & Poston, K. (2017, January 1). The quest for privacy. *Strategic Finance*,25–41.

Barucci, E., Landi, L., & Cherubini, U. (1996). Computational methods in finance: Option pricing. *IEEE Computational Science and Engineering*, *3*(1), 66–80. [CrossRef]

Binder, J. (1998). The event study methodology since 1969. *Review of quantitative Finance and Accounting*, *11*(2), 111–137.

Coderre, D. G. (2000). Computer assisted fraud detection. *Internal Auditor*, *57*(4), 25.

Cohen, J. A. (2011). *Intangible assets: Valuation and economic benefit*. Hoboken, NJ: John Wiley & Sons, Vol. 273.

Cox, E. (1992). Integrating fuzzy logic into neural nets. *AI Expert*, *7*(6), 43–47.

Credeur, M. J. (2012, February 6–12). Marriage at 30,000 Feet. *Businessweek*, 58–63.

Deming, W. E. (1993). *The new economics: For industry, government, education*. Cambridge: MIT Press.

Eining, M. M., Jones, D. R., & Loebbecke, J. K. (1997). Reliance on decision aids: An examination of auditors' assessment of management fraud. *Auditing: A Journal of Practice & Theory*, *16*(2), 1–19.

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The adjustment of stock prices to new information. *International Economic Review*, *10*(1), 1–21. [CrossRef]

Gutierrez, I., & Carmona, S. (1988). A fuzzy set approach to financial ratio analysis. *European Journal of Operational Research*, *36*(1), 78–84. [CrossRef]

Harrison, W. T. Jr., Horngren, C. T., & Thomas, C. W. (2017). *Financial Accounting* (11th ed.). Upper Saddle River: Pearson.

Hruschka, H. (1988). Use of fuzzy relations in rule-based decision support systems for business planning problems. *European journal of operational research*, *34*(3), 326–335. [CrossRef]

Khazanchi, D., & Arora, V. (2016). Evaluating Information Technology (IT) Integration Risk Prior to Mergers and Acquisitions (M&A). *ISACA Journal*, *1*, accessed online via https://www.isaca.org/Journal/archives/2016/Volume-1/Pages/evaluating-it-integration-risk-prior-to-mergers-and-acquisitions.aspx.

Koller, G. (2005). *Risk assessment and decision making in business and industry: A practical guide*. Boca Raton, FL: CRC Press.

Kryzanowski, L., Galler, M., & Wright, D. W. (1993). Using artificial neural networks to pick stocks. *Financial Analysts Journal*, *49*(4), 21–27. [CrossRef]

Levy, J., Mallach, E., & Duchessi, P. (1991). A fuzzy logic evaluation system for commercial loan analysis. *Omega*, *19*(6), 651–669. [CrossRef]

Lin, J. W., Hwang, M. I., & Becker, J. D. (2003). A fuzzy neural network for assessing the risk of fraudulent financial reporting. *Managerial Auditing Journal*, *18*(8), 657–665. [CrossRef]

McWilliams, A., & Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, *40*(3), 626–657.

Oler, D. K., Harrison, J. S., & Allen, M. R. (2008). The danger of misinterpreting short-window event study findings in strategic management research: an empirical illustration using horizontal acquisitions. *Strategic Organization*, *6*(2), 151–184. [CrossRef]

Piramuthu, S. (1999). Financial credit-risk evaluation with neural and neurofuzzy systems. *European Journal of Operational Research*, *112*(2), 310–321. [CrossRef]

Port, O., & Raeburn, P. (1999, December 6). AI in the air conditioning. *Business Week*, 83.

Raschke, R. L. (2010). Process-based view of agility: The value contribution of IT and the effects on process outcomes. *International Journal of Accounting Information Systems*, *11*(4), 297–313. [CrossRef]

Reber, G. (2017, October 12). How to Buy Cyber Insurance. CFO.com. Retrieved from http://ww2.cfo.com/it-security/2017/10/buy-cyber-insurance.

Rohrer, K., & Hom, N. S. (2017). Who's responsible for cybersecurity. *Strategic Finance*, *99*, 62–63.

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly*, *27*(2), 237–263. [CrossRef]

Siddique, N., & Adeli, H. (2013). *Computational intelligence: Synergies of fuzzy logic, neural networks and evolutionary computing*. Hoboken, NJ: John Wiley & Sons.

Sorescu, A., Warren, N. L., & Ertekin, L. (2017). Event study methodology in the marketing literature: An overview. *Journal of the Academy of Marketing Science*, *45*(2), 186–207. [CrossRef]

Tam, K. Y., & Kiang, M. Y. (1992). Managerial applications of neural networks: the case of bank failure predictions. *Management Science*, *38*(7), 926–947. [CrossRef]

Tanaka, H., Okuda, T., & Asai, K. (1976). A formulation of fuzzy decision problems and its application to an investment problem. *Kybernetes*, *5*(1), 25–30. [CrossRef]

Tarasovich, B., Lyons, B., & Gerlach J. (2008). After the acquisition. *Strategic Finance*, *90*(4), 25–31.

Trippi, R. R., & Turban, E. (1996). *Neural networks in finance and investing: Using artificial intelligence to improve real world performance*. New York: McGraw-Hill, Inc.

Turban, E., & Aronson, J. (2000). *Decision support systems and intelligent systems* (6th ed.). Englewood Cliffs: Prentice-Hall.

Turunen, I., Järveläinen, M., & Dohnal, M. (1984). Fuzzy approach to factorial cost estimation of chemical plants. *Engineering Costs and Production Economics*, *7*(4), 279–292. [CrossRef]

Wessel, M., Allworth, J., & Levie, A. (2015). Old management systems stifle new business models. *Harvard Business Review*, *4*, 2.

Wong, F. S., Wang, P. Z., Goh, T. H., & Quek, B. K. (1992). Fuzzy neural systems for stock selection. *Financial Analysts Journal*, *48*(1), 47–52. [CrossRef]

Zadeh, L. A. (1965). Fuzzy Sets. *Information and Control*, *8*(3), 338–353. [CrossRef]