Risk Management and Business Valuations

By Raymond Hutchins and Dave Miles, CPA, CVA, CGMA (Originally published in the Value Examiner)

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Contents

It is rare and notable when anything new hits the valuation industry. But that moment has come. Cybersecurity due diligence must now be part of any new business valuation. To ignore this new reality invites unnecessary credibility challenges, liability, and litigation.

The Problem

Cybersecurity risk applies to all businesses today. While valuators might think that cybersecurity applies only to larger enterprises, that is incorrect. The internet has created a playing field where size does not matter. Small businesses are using technology every day in completing their tasks, whether it is making a call on a smart phone or using e-mail. Many smaller business owners mistakenly believe that installing a firewall or using antivirus software is enough protection because their companies are small and do not have any "valuable" data. Cybersecurity breaches do not discriminate based on size. Cyber thieves look for opportunity. Small businesses are just as likely to have a cybersecurity breach as large ones—and they have far fewer resources to deal with one when it happens.

In today's world, cybersecurity (like accounting) is a business process that permeates every area of the business. Accounting is a part of the sales cycle; so is cybersecurity. Accounting is a part of the supply cycle; so is cybersecurity. Accounting is a part of the manufacturing process; so is cybersecurity. The point is simple. If a valuation professional gets a bad feeling about accounting, the value of the business is questioned. Likewise, if the valuation professional gets a bad feeling about the cybersecurity, the value should be affected.

It is not required that valuation professionals be cybersecurity experts. Valuation experts are smart enough to understand that a risk exists, and it should be quantified or excluded from the valuation scope. Obviously, "it depends" comes into play.

If the costs to mitigate or correct the breach are minimal, then there is less of a problem. However, if those costs are substantial, then the reverse is true.

The first takeaway is exactly this: in the limiting conditions or scope limitation of the report, there should be a statement about cybersecurity. At the extreme end, a limiting condition should disclose that cybersecurity risk was not considered and that it may have a material impact on the value of the business. If cybersecurity is considered, the limiting condition can be softened to be in sync with the work performed.

Cybersecurity: A key consideration in any business valuation

It is accepted that risk affects valuation, but only recently has it been recognized that cybersecurity is a pervasive risk. Once insurance companies started selling cybersecurity insurance, any arguments to the contrary were stilled. The fact that there is a burgeoning market for cybersecurity insurance is validation that cybersecurity is a real risk. It could be the subject of an entire article, but cybersecurity insurance is not a "get out of jail free card" for dealing with cyber risk. It is the last resort. And, cybersecurity insurance has many landmines of its own because it is a non-standard form policy.

In today's world, most businesses are forced to operate on top of an IT infrastructure that is inherently insecure. Not every business must use this IT infrastructure to move and store sensitive data, but for most businesses, that is the reality. In today's world: The greater the dependence upon the IT infrastructure to operate the business, the greater the risk.

If a business cannot effectively defend its IT systems and data from attack, then it is worth less than a business that can defend itself. It is the valuation professional's job to define the impact of cybersecurity risk on that valuation.

Nowadays, in addition to other valuation factors, a company's value is directly related to the value of different types of data:

- Intellectual Property Data
- Client Data
- Application(Software) Data

Additionally, that value is impacted by the amount of unmitigated cybersecurity risk, including:

- Accessibility to that data
- Security of that data
- Safety and security of the systems required to use that data
- Commitment to security by the people controlling that data

If a valuator is not aware of these issues and does not ask questions related to these issues, then how can the valuator establish the company's true value? And remember, nondisclosure of cybersecurity risk is no longer an option.

Case Studies

Let's look at several real-life examples that will demonstrate the point—some larger companies and then some smaller companies. Note that larger companies are more likely able to survive breach events because they have resources to deal with a breach, while smaller companies may have to file for bankruptcy protection or dissolve.

Target Breach, December 2013

We will not discuss how the breach happened, but forty million credit cards plus an additional seventy million customer loyalty cards were stolen. Target paid nineteen million dollars in fines and another $154 million in legal settlements. Their 2016 annual report said that total financial cost to the company was $292 million—less a $100 million cyber insurance payment.

The event occurred in 2013, and it is still not resolved; hard costs continue to accrue as of 2019.

But what is the cost of being distracted by litigation for five to ten years? What is the unfunded liability? How has this impacted Target's value? The stock price took a major hit immediately after the breach but has since recovered. This is because the target had major resources to respond that a smaller enterprise would not have.

Verizon Purchase of Yahoo, 2013–2014

During Verizon's due diligence process in purchasing Yahoo during 2013–2014, Verizon accidentally discovered a breach of Yahoo's systems. The personal data of three billion account holders were exposed, but no credit card info was exposed.

As a result of this breach, Verizon reduced the purchase price from $4.8 billion to $4.48 billion and demanded that Yahoo shareholders pay costs associated with remediation, loss of customers, business disruption, regulatory fines, legal costs, etc. Yahoo shareholders also had to set aside monies to cover retained liability associated with this breach.

While the sale ultimately went through, as of 2019, the matter is still not fully settled.

Marriott's Acquisition of Starwood and Sotheby's Acquisition of Home

Both of these acquisitions occurred in late 2018, and in both cases, hackers had been operating undetected inside the IT systems of the companies being acquired for years. In both cases, the hackers were not detected until years after the acquisitions were completed.

In neither case was there any hold-back for cyber issues nor any retained liability in the sale documents. The new buyers just had to absorb all negative impacts.

Microsoft Purchase of a Small Company for Ten Million Dollars

During the purchase, Microsoft did not perform good cybersecurity due diligence and discovered various cybersecurity network and application vulnerabilities after the sale had closed. Microsoft was forced to mitigate all the problems, and it cost them ten million dollars to do so.

They paid double for the acquisition.

The only saving grace was that there was no breach of the systems or public data involved, or it would have been worse. But from a valuation point of view, this was a disaster.

Deal Killed Because of Poorly Built Software

This was a company acquisition that CyberCecurity LLC partner, Mitch Tanenbaum, personally witnessed.

In 1996, the financial services company Mitch worked for purchased another company for three million dollars. The primary reason they wanted to buy the company was to get ownership of a key piece of software that was core to its business.

But the buying company failed to request adequate access to that software to conduct proper cyber due diligence. When the software was originally developed, the developers did not use a

secure software development lifecycle process. Therefore, the software application was completely

not secure, impossible to maintain, and vulnerable to attack (by the way, the vast majority of legacy software in use today falls into this category).

By the time the purchasing company discovered their error, the transaction had already been funded. It was determined that the cost to review the code, remediate the coding errors, and put into place a company-wide cybersecurity program, would have been one million dollars or thirty-three percent of the original valuation of three million dollars.

In this case, the buying company was able to reverse the transaction and get their money refunded due to a threat of litigation.

After that, the buyer was not willing to stay in the deal because they did not know if sensitive data had already been stolen and/or compromised by competitors.

Benefits to Clients Considering Cybersecurity in Valuations

When valuators include cybersecurity due diligence as part of your valuation process, you do the following:

- Provide a more accurate valuation of the business
- Help the client protect and increase the value of their business
- Help the client better understand and protect their data
- Help the client better understand and protect their money and assets

Benefits to Valuators By Considering Cybersecurity in Valuations

While the conversation may be unexpected and somewhat psychologically painful, benefits accrue to valuators as well. They are:

- Reducing the risk and liability associated with valuations that do not factor in cybersecurity
- Bringing more value to your clients
- Increasing and protecting the value of your practice
- Gaining a competitive edge

How to Determine Whether Cybersecurity is a Valuation Factor

While it is certainly true that virtually all businesses today are built upon an insecure IT infrastructure, not all businesses are vulnerable to attack and material financial loss. For example, restaurants that use secure third-party Point-of-Sale (POS) systems could be reasonably immune to attack if they do not directly collect and store customer data. Their IP (recipes and business processes) may be exposed and should be protected, but the remediation of this issue might be fairly inexpensive and fast.

To determine if you have a cybersecurity risk, it is important to ask several important questions that help you decide if you are in danger of a cybersecurity breach.

Ten Cybersecurity Valuation Test Questions

1. Does the company have sensitive data that it is responsible for protecting, and that might be of value to competitors, criminals, or foreign governments (intellectual property, client data, non-public personal information)?
2. Is the business in compliance with applicable state, federal, or professional cybersecurity/privacy laws or requirements (HIPAA, PCI, various privacy laws, and others)?
3. Does the business have a significant online presence?
4. Does the company develop and/or maintain online applications that collect sensitive information, or which are crucial to the operation of the business?
5. Does the company have a written cybersecurity program?
6. Is an executive-level employee responsible for this program?
7. Would a cyber incident that affected the company's reputation impact the value of the company?
8. Would the company be negatively impacted if their online systems (internal or public) were taken out of service for a week or a month due to a cyber incident?
9. What kind of cybersecurity insurance does the company carry?
10. Has the company ever had a cyber incident (virus, ransomware, business e-mail compromise, wire fraud, breach of NPI)?

These ten questions should help to decide the extent of the risk cybersecurity present. If the risk is small or immaterial, it might be ignored.

But if the risk is determined to be unquantifiable, then a third-party expert should be consulted. And if the risk is large and quantifiable, then the valuation professional should consider that fact in the development and reporting of a conclusion of value.

Cybersecurity Risk in Development Standards

In the Asset Approach, can you identify intellectual property that needs to be protected? Is there a risk to computer systems and technology that would affect value? If there is a risk, and it is material, an expert might be sought out to determine how much it would cost to mitigate the risk and the value adjusted accordingly, i.e., treated as an off-balance sheet liability. The hypothetical buyer would do this.

In the Income Approach, the discount rate should be adjusted or a direct adjustment to value made. Typically, when company-specific risk is assigned, different characteristics are listed. Based on the ten questions asked in an interview, cybersecurity should be one of the characteristics. Furthermore, if the costs to control and mitigate the risk are known, a direct adjustment to value would be appropriate. Perhaps, cash flow would be adjusted to show the ongoing cost of

cybersecurity

The Market Approach becomes interesting. Did the comparable transactions consider cybersecurity risk? Does cybersecurity create a material change in the multiplier? As experts, the data you choose to use must be understood and used accordingly. The additional value of strong cybersecurity and the downward adjustments to value for weak cybersecurity are recent developments. We believe that the expert should decide the best approach but start with the cost to mitigate as a decrease to the value of the subject company.

SECURITY BREACHES IN THE NEWS

In July 2019, just before The Value Examiner went to press, It was revealed that a hacker gained access to more than one-hundred million Capital One customers' accounts and credit card applications earlier this year. According to the bank and the US Department of Justice, the accused hacker, Paige Thompson, gained access to 140,000 Social Security numbers, one million Canadian Social Insurance numbers and 80,000 bank account numbers, in addition to an undisclosed number of people's names, addresses, credit scores, credit limits, balances, and other information.

In the same month, Equifax, the credit rating company, announced a settlement agreement with regards to its data breach, which occurred in September 2017. One hundred forty-seven million consumers were affected. Hackers were able to get access to a multitude of consumer private information, including names, Social Security numbers, dates of birth, credit card numbers and even driver's license numbers.

During the investigation into the breach, Equifax admitted the company was informed in March that hackers could exploit a vulnerability in its system, but failed to install the necessary patches. As part of the settlement agreement, Equifax will also pay $175 million in civil penalties to states, and a $100 million fine to the Consumer Financial Protection Bureau.

According to experts in cybersecurty such as George Wrenn, CEO of Cybersaint, a company based in Boston, MA, these breaches are an example of when an organization does not practice integrated risk and compliance. According to Wrenn, challenge for many of these enterprises - especially those like Capital One that process such sensitive information - is ensuring that they have the infrastructure in place to be aware when a vulnerability like this exists or a control fails… There needs to be a greater awareness across the entire organization, and especially within the information security organization, that these kinds of breaches directly impact their customers as well as directly impact the business' bottom line."

Nancy McCarthy, Senior Editor, The Value Examiner

Cybersecurity Risk in The Reporting Standards

There are three areas where this risk must be identified if it exists and a fourth if an outside expert is used. The first discussion is in the limiting conditions or scope limitations where the risk is identified and its effect on the results quantified. The second discussion is in the description of the company and how it does business where the risk is identified. The third discussion is in the valuation method used where the value adjustment is made. Lastly, if a third-party specialist is used, the report discussion should disclose what reliance was placed upon that work and who is responsible for the work done by the specialist.

Conclusion

While it is not necessary to be a cybersecurity expert, cybersecurity may now have a material impact on valuation. The magnitude of this impact can be determined by addressing cybersecurity in the management interview, the development of a value, and the reporting of a value.

Did you find this position paper of value? Here are some of our other papers.

- IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
- Secrets of Hiring and Firing vCISOs
- GLBA & FTC Safeguards Rule
- Hiring, Managing and Firing MSPs

Raymond Hutchins is the managing partner for CyberCecurity LLC, a full-service cybersecurity and privacy firm headquartered in Denver, Colorado that has an international client base. He and his partner, Mitch Tanenbaum, have over fifty years of IT, cybersecurity, and privacy experience. They are highly respected national cybersecurity leaders who speak and write frequently on the subject of cybersecurity, privacy, and compliance. They are the first cybersecurity professionals to introduce cybersecurity due diligence to the accounting and valuation professions. E-mail: rh@cybercecurity.com

Dave Miles, CPA, CVA, CGMA, is the business valuation manager at ValuSource. For the last nineteen years, he has worked on developing software, developing web applications, publishing datasets, and providing valuation expertise to both customers and the ValuSource team. Typically, he identifies the "what" and "why" of a valuation technique or database and then passes on that knowledge. E-mail: dmiles@valusource.com

© 2025 Copyright CyberCecurity, All rights reserved.