Cyber Risk Profile of a Merger or Acquisition

Tyler Whittington

Cyber Risk Profile of a Merger or Acquisition

GIAC (GSLC) Gold Certification

Author: Tyler Whittington, ltwhit@pm.me
Advisor: Russell Eubanks

Accepted: 04/12/2021

Abstract

Companies often use mergers and acquisitions to expand their market share and increase profitability. To appropriately assess a potential target, acquiring companies regularly dedicate time and resources to identify risks and quantify the target company's value. A company's cyber risk is not commonly considered a factor in pre-acquisition assessments, nor does an organization's Information Security team frequently play an active role in this process.

Due to these gaps, acquiring companies have identified incidents both during and after an acquisition deal has closed. These late discoveries resulted in millions of dollars in lost revenue and or breaches affecting millions of customers. Advancements within the Information Security industry have enabled the collection of open-source information through tools and standardized reconnaissance methodologies. Based on these accomplishments, research must be conducted to determine how this information can be used to calculate a company's cyber risk without the benefits of internal visibility.

1. Introduction

According to the Institute for Mergers, Acquisitions, and Alliances (n.d.), the total global value of merger and acquisition (M&A) deals reached over 3.3 trillion U.S. dollars in 2019. Organizations spend months to years assessing target companies to identify a candidate that will maximize revenue at an acceptable level of risk to stakeholders. However, companies frequently initiate contracts containing unknown cyber risk, which can lead to devaluation and transferred risk. Organizations such as Softbank, Verizon, and Equifax are a few organizations that have identified incidents following initiated M&A deals, which impacted millions of newly acquired customers (Jelen, 2019).

Haspeslagh and Jemison (1991) noted the M&A process is divided into four phases: the idea, acquisition justification, acquisition integration, and results. Figure 1 details the four phases of the M&A process.

Figure 1. Phases of the M&A process

Information Security teams are often engaged well after contracts have been finalized and primarily to facilitate the acquisition integration. Gartner predicted 60% of companies will include Information Security as part of their M&A acquisition justification process by 2022, but the current number is around 5% (Olyaei, 2018). As Jemison and Sitkin (1986) noted, "[Top Executives] need to search for ways to structure a balance among different groups and interests to ensure an integrated set of analyses." By doing so, the company is more likely to "realize its broader strategic goals in the acquisition" (Jemison & Sitkin, 1986).

While organizations are generally limited by legal and regulatory governance as to what information can be shared with the market, companies may also choose to be less

forthcoming about information that may be detrimental to a potential offer or favorable valuation of their assets. For example, Uber hid the details of a 2016 data breach for one year before going public for the first time (Chappell, 2018). As a result, companies need a framework to create a risk profile of an M&A candidate based on publicly available information.

This research will create a framework to establish an information baseline, which is publicly obtainable, that will be used to gain valuable insight into a company's cyber risk. Public information is defined as any information available through the Internet without illegal or otherwise obtrusive acquisition. By utilizing free tools[1], this study can provide a methodology that may otherwise be cost-prohibitive for companies interested in utilizing this framework.

Additionally, the framework will demonstrate how different tools can be used to collect this public information. By examining the tools' output utilizing a custom qualitative risk rating methodology, the study will provide a repeatable method to assess target companies while also permitting flexibility based on the stakeholders' cyber risk tolerance.

Publicly available information will be unique to the target. This study's experiment will attempt to establish this framework's limitations by identifying multiple companies across different industries and varying sizes. Then, each company will be investigated and rated based on the framework.

This framework cannot account for every vulnerability and threat, as it will rely on public data. Public data can be manipulated and obfuscated either directly or indirectly. Despite this limitation, companies should take every available avenue to develop cyber risk assurance before finalizing an M&A deal. The framework's success will be demonstrated by creating accurate and meaningful cyber risk profiles for organizations regardless of their size, industry, and general notoriety.

[1] Referenced tools may provide additional capabilities at cost, but this study will be limited to free capabilities.

Tyler Whittington, ltwhit@pm.me

2. Target Information

2.1. Security Incidents

On security incidents, Bromiley (2019) noted, "Previous incidents provide insight into what was possible before. If left unmitigated, these risks may pop up again." While companies should take precautions to prevent repeat security incidents, the companies may needlessly limit the scope of what to remediate following an incident. For example, a company with an unauthorized, externally available RDP[2] service may limit remedial activities to identifying and closing unnecessary RDP access across their environment. However, this gap may indicate a more significant issue with firewall access controls and could lead to additional opportunities for threat actors. On the other hand, some companies may overcompensate after a singular, publicized incident by focusing on one root cause while neglecting other contributing factors. When assessing potential M&A targets, acquiring companies should look at past security incidents to identify the target's security trends.

2.2. Threat Intelligence

Threat actors maintain tactics, techniques, and procedures, which allow analysts to establish trends. When security researchers communicate these details to the public, companies can correlate this information with other intelligence. Even if an organization has not been a victim itself, industry trends can also be applied to proactively assess unrealized threats. Bromiley (2019) states, "By taking techniques…and associating them with a particular group, your organization can start to discover where you could or could not detect a threat actor within your environment." This same approach can be used by third parties, such as acquiring companies, to gain insights into a target company.

[2] RDP, also known as the Remote Desktop Protocol, is a service that provides a connection to another computer over a network.

2.3. Perimeter Mapping

Lockheed Martin's Cyber Kill Chain revolutionized the security industry by outlining the methodology threat actors use to conduct cyberattacks. The first step, reconnaissance of a target, is the building block from which all operations are initiated (Hutchins et al., 2011, p. 4). More specifically, reconnaissance can be defined as the study of a target's perimeter. Within this study, a company's perimeter is defined as any system or application exposed to the Internet. These company assets provide indispensable insights into the maturity of a security program even through passive observations. Furthermore, researchers can also maintain anonymity through this process, which is integral to the pre-acquisition process. An M&A news leak, however indirect, "could cause disruptions internally or in the financial markets" (Jemison & Sitkin, 1986).

3. Data Sources and Tools

3.1. Security Incidents

Businesses consider regulatory governance, industry best practices, and internal risk tolerance when identifying and classifying security incidents. Additionally, organizations could have varying external reporting requirements for security incidents. Organizations may have different perspectives and stances on what constitutes a security incident and what is disclosed as a result.

The security industry has introduced numerous taxonomies through standardized definitions and categories to reduce variance. As an example, Verizon created the Vocabulary for Event Recording and Incident Sharing (VERIS) framework as a "common language to describe the series of events compromising a security incident" (Verizon, 2017). Without enforced conformity to a single standard, businesses will likely continue to diverge in their approach. Security researchers and news organizations may also report and archive security incidents based on different criteria due to these circumstances. In summary, multiple sources will need to be consulted to identify publicly reported security incidents for a target company.

Following VERIS, Verizon rolled out the VERIS Community Database (VCDB). The Verizon RISK team organized the VCDB as a research repository for security incidents reported by volunteers (Verizon RISK, 2013). Researchers can access the data through a GitHub repository[3]. The VCDB community documents security incidents in alignment with the VERIS framework and emphasizes correctness, consistency, and completeness. The VERIS framework describes incidents based on threat actions, type of compromised assets, and security attributes. Through these records, companies may clarify incident details where traditional reporting may lack sufficient information. Additionally, the Verizon RISK team allows the community to include security incidents without a data breach component, such as Denial of Service (DOS) attacks or website defacements. The VCDB developers caution that incidents such as "healthcare issues and some priority issues" are selected at random with additional consideration for incidents within the last year (Verizon RISK, 2014).

Victim organizations may share security incident details on their external websites and through various communication platforms. For example, SolarWinds provided details of their SUNBURST and SUPERNOVA security incidents through continuous updates on their external website (SolarWinds, 2021). However, as previously mentioned, organizations limit the scope and details of information shared about security incidents. Therefore, researchers should consult multiple sources, where possible, to ensure conclusions are based on complete, objective data.

3.2. Threat Intelligence

Researchers will not frequently identify direct connections to a target company based on threat intelligence. As Bromiley (2019) stated, "Intelligence sources may also be industry- or company-specific and give you an ideal starting point." Unlike security incidents and perimeter mapping, threat intelligence relies heavily on predictive analysis through strong correlations and trends observed across the Internet. Effective threat

[3] The repository is located at https://github.com/vz-risk/VCDB.

intelligence processes ensure sufficient coverage to collect actionable information while simultaneously reducing irrelevant noise.

One potential source for threat intelligence is the SANS Internet Storm Center (ISC), which serves as a "free analysis and warning service to thousands of internet users and organizations" (SANS Institute, n.d.-a). Volunteers maintain the ISC by analyzing threats and disseminating information to the public. The service provides insights into threats across the globe based on user-submitted data, such as firewall logs, and centralizes threat intelligence from other public sources. From this data, users can gather information based on several criteria, such as keywords, domains, ports, IP addresses, and network service banners. The ISC service also provides a risk score calculated based on the number of targets, external threat feeds, user-submitted data, and other criteria (SANS Institute, n.d.-b).

3.3. Perimeter Mapping

Due to the lack of a single source of truth for consolidated information on a company, researchers must often apply iterative approaches to map a company's perimeter when provided with new sources and data. Reconnaissance tools attempt to address this issue by tapping into multiple resources while also reducing repetitive search techniques. When used effectively, acquiring companies can prioritize their effort and resources into more obscure and indirectly sourced intelligence.

One solution is Maltego, a robust analysis tool, which collects information through open-source data and shows relationships using graphs. The GUI-based tool classifies information into "entities" and relies on operations known as "transforms" to gather information in a repeatable manner. With the addition of transforms to further uncover the connections between entities, researchers can create standardized, automated processes to quickly reveal new connections of individuals, systems, applications, and organizations. The Maltego non-commercial Community Edition can be installed as a desktop client on Windows, Linux, and Mac Operating Systems (See Appendix: Maltego System and Network Requirements). In order to use the software, users must also create a free Maltego Community Edition account.

Tim Tomes developed Recon-ng to perform web-based open-source reconnaissance (Offensive Security, n.d.). The tool utilizes SQL databases to store and modify information as necessary. Modules, created and maintained by the user community, provide specific capabilities, which can be included based on the researcher's use case. Most modules require credentials such as API keys to access third-party resources to expand the tool's extensibility. Potential Recon-ng users should note some third-party resources require a one-time fee or paid subscription.

Unlike many free tools, Recon-ng provides several quality-of-life enhancements to reduce the burden of managing investigations for multiple targets. These features include, but are not limited to, command recording, configuration persistence, and automation support. Another practical feature, Recon-web, provides a web interface to create data visualizations and reports from stored data sets.

4. Risk Profiling Framework

4.1. Risk Calculation

The framework will assign a qualitative risk rating to a company based on the three areas mentioned earlier: security incidents, threat intelligence, and perimeter mapping. Each area contains different categories (column) and related criteria (row). Each criterion is assigned a score of 0 – 3, with three as the highest risk. The average score for all the criteria will represent the area's score. Each score will then be combined to determine the company's overall risk rating. Figure 2 indicates the risk rating based on a company's overall score.

Company Risk Rating	
Score	**Risk**
7 – 9	High
4 – 6	Medium
1 – 3	Low
0	Unknown

Figure 2. Company Risk Ratings and Scoring

4.1.1. Security Incidents

This framework selected broad, general criteria for security incidents to remove subjective bias inherent to companies and industries. For example, companies in the financial sector are more likely to face stricter regulatory controls than a healthcare provider. However, security incidents disrupting critical healthcare services could result in fatalities. Each industry maintains various justifications for prioritizing its incidents, but this framework's scope does not include tailored criteria for every industry and use case. Figure 3 indicates the criteria for security incidents and associated risk score.

	Security Incidents			
	Categories			
	Incident Type	**Incident Impact**	**Incident Volume**	**Score**
Criteria	Information breach or long-term outage to business operations	Catastrophic	Multiple security incidents	3
	Temporary disruption to business processes or services	Moderate	One security incident	2
	Local, isolated event	Insignificant	No security incidents	1
	Unknown	Unknown	Unknown	0

Figure 3. Criteria for Security Incidents

4.1.2. Threat Intelligence Scoring

When assessing organizations based on current and potential threats, acquiring companies can look at previous security incidents and threat intelligence within the broader industry and sectors. Since predictive modeling is often used to create threat intelligence, researchers may draw incorrect conclusions from limited information. Where possible, pattern analysis should be applied to increase the credibility of a predictive assessment. Figure 4 indicates the criteria for threat intelligence and associated risk score.

	Threat Intelligence			
	Categories			
	Threat Motivation	**Threat Capabilities**	**Threat Frequency**	**Score**
Criteria	Threat actor(s) conduct attack(s) that require extended planning and execution, such as espionage and ideology-based attack(s)	Threat actor(s) exhibit advanced techniques and resources common to state-sponsored groups	Attack(s) are carried out over extended, targeted campaigns	3
	Threat actor(s) are focused on short-term results, such as monetary gain or revenge	Threat actor(s) demonstrate the ability to create custom exploits as necessary	Attack(s) occur semi-frequently but do not indicate coordinated efforts	2
	Threat actor(s) are not motivated by any specific goal or target	Threat actor(s) rely on weak security controls or techniques with inconsistent success	Attack(s) are isolated to random windows of opportunity and follow no patterns or trends	1
	Unknown	Unknown	Unknown	0

Figure 4. Criteria Scoring for Threat Intelligence

4.1.3. Perimeter Mapping

Since perimeter mapping focuses on identifying and analyzing Internet-facing assets, target companies will be assessed based on the risk surrounding these systems and applications. Asset function and valuation have been normalized using qualitative

descriptions and ranges to ensure consistent conclusions regardless of company size and industry. Asset exposure requires a general understanding of security architecture and industry best practices to determine the intended asset availability against the discovered level of exposure. Figure 5 indicates the criteria for perimeter mapping and associated risk score.

	Perimeter Mapping			
	Categories			
	Asset Function	**Asset Valuation**	**Asset Exposure**	**Score**
Criteria	System(s) or application(s) that stores sensitive information or performs critical business functions	Major	External users can directly access internal system(s)	3
	System(s) or application(s), which if disrupted, may cause minimal to moderate impact to the business	Minor	External users have visibility of internal system(s) information, including system configurations	2
	System(s) or application(s), which if disrupted, have no impact to the business	None	External user(s) have limited to no visibility of internal assets	1
	Unknown	Unknown	Unknown	0

Figure 5. Criteria Scoring for Perimeter Mapping

4.2. Test Case Selection Criteria

Acquiring companies hold different perspectives of a potential M&A candidate based on their size. Inversely, a target company's size is subjective based on the acquiring company. This framework will use the United States' size definitions to differentiate between a small and large business to minimize subjectivity in interpretation. The U.S Small Business Administration (n.d.) maintains size standards based on the business' industry, number of employees, and gross income.

In addition to size as a selection criterion, the study will select test cases from different industries as defined by the North American Industry Classification System (NAICS)[4]. Industries face starkly different challenges when comparing the volume of publicly reported security incidents. To further demonstrate, Figure 6 includes a table with the number of businesses[5] per industry[6] and the number of security incidents[7] per industry[8] as reported[9] in Verizon's 2020 DBIR (Verizon, 2020).

Industry	Number of Businesses	Total Number of Incidents
Accommodation and Food Services	913,929	217
Administrative and Support and Waste Management and Remediation Services	1,662,201	47
Agriculture, Forestry, Fishing, and Hunting	382,038	52
Arts, Entertainment, and Recreation	379,799	292
Construction	1,526,509	62
Educational Services	431,622	1,047
Finance and Insurance	792,376	1,957

[4] The NAICS is a "production-oriented, or supply-based, conceptual framework," which assigns companies with 2- to 6-digit codes (NAICS Association, n.d.-a)

[5] The NAICS Association reported the number of businesses per industry based on Dun & Bradstreet's figures from October 2020 (NAICS Association, n.d.-b).

[6] Some industries, such as Educational Services and Utilities, include both public and privately-owned organizations. As a result, these metrics should not be considered exclusive to private companies.

[7] Verizon defines security incidents and breaches as separate events and provides metrics based on those definitions. These metrics have been combined for this table.

[8] Metrics for Public Administration and incidents without a specified industry have been omitted.

[9] Individual businesses may experience multiple security incidents and breaches, inflating the total number for the industry.

Health Care and Social Assistance	1,778,521	1,319
Information	368,730	5,831
Management of Companies and Enterprises	75,714	54
Manufacturing	643,451	1,303
Mining	32,529	63
Other Services (except Public Administration)	1,947,031	173
Professional, Scientific, and Technical Services	2,370,906	7,789
Real Estate Rental and Leasing	891,450	70
Retail Trade	1,824,281	433
Transportation and Warehousing	614,334	179
Utilities	47,917	174
Wholesale Trade	701,077	40

Figure 6. Number of Businesses and Security Incidents per Industry

Based on Figure 6, researchers may conclude the Information industry contains the highest number of incidents per business. However, security researchers may artificially inflate the reported numbers towards their industry[10]. The experiment will include companies from different industries as an additional independent variable in hopes of offsetting this potential bias. Figure 7 includes the details of each company selected as a test case.

[10] Verizon, classified under the Information industry, reported the cited security incident numbers.

Company	Industry Title (as per NAICS)	NAICS Code	Company Size (as per SBA)
Anytime Fitness	Arts, Entertainment, and Recreation	713940	Large
Comcast Corporation	Information	515210 517911	Large
Peachtree Neurological Clinic, PC	Health Care and Social Assistance	621111	Small
Seidl's Party Supplies & Rental	Real Estate Rental and Leasing	532189	Small

Figure 7. Test Cases and Details

5. Analysis

5.1. Anytime Fitness

VCDB recorded one incident, which occurred in 2019, for the company. The incident summary indicated an isolated incident involving two disgruntled employees. The two individuals maliciously canceled existing memberships at an estimated $13,000 loss to the company, in addition to other financial damages. Prosecutors charged the former employees with fraud, theft, and computer tampering. Additional research using search engines and the company's website did not yield information of additional security incidents. Figure 8 indicates the criteria for security incidents and the company's average risk score (highlighted).

	Security Incidents			
	Categories			
	Incident Type	**Incident Impact**	**Incident Volume**	**Score**
Criteria	Information breach or long-term outage to business operations	Catastrophic	Multiple security incidents	3
	Temporary disruption to business processes or services	Moderate	One security incident	2
	Local, isolated event	Insignificant	No security incidents	1
	Unknown	Unknown	Unknown	0

Figure 8. Anytime Fitness Score for Security Incidents

Through results collected from perimeter mapping, it was discovered that the company has 37 public assets. Research of the IP addresses for these assets against the SANS ISC revealed no additional information. Although isolated, the previously referenced incident did indicate threat actors were motivated by a grudge against the company, and they exhibited amateur skills to access company assets. Figure 9 includes the criteria for threat intelligence and the company's average risk score (highlighted).

	Threat Intelligence			
	Categories			
	Threat Motivation	**Threat Capabilities**	**Threat Frequency**	**Score**
Criteria	Threat actor(s) conduct attack(s) that require extended planning and execution, such as espionage and ideology-based attack(s)	Threat actor(s) exhibit advanced techniques and resources common to state-sponsored groups	Attack(s) are carried out over extended, targeted campaigns	3
	Threat actor(s) are focused on short-term results, such as monetary gain or revenge	Threat actor(s) demonstrate the ability to create custom exploits as necessary	Attack(s) occur semi-frequently but do not indicate coordinated efforts	2
	Threat actor(s) are not motivated by any specific goal or target	Threat actor(s) rely on weak security controls or techniques with inconsistent success	Attack(s) are isolated to random windows of opportunity and follow no patterns or trends	1
	Unknown	Unknown	Unknown	0

Figure 9. Anytime Fitness Score for Threat Intelligence

Based on the company's website, www[.]anytimefitness[.]com, Recon-ng identified 37 public assets. No internal assets were discovered. Shodan[11] did not identify any vulnerabilities of the company's assets, which would have allowed further visibility or access into their internal network. Figure 10 includes the criteria for perimeter mapping and the company's average risk score (highlighted).

[11] Shodan is a search engine for Internet-connected devices.

	Perimeter Mapping			
	Categories			
	Asset Function	**Asset Valuation**	**Asset Exposure**	**Score**
Criteria	System(s) or application(s) that stores sensitive information or performs critical business functions	Major	External users can directly access internal system(s)	3
	System(s) or application(s), which if disrupted, may cause minimal to moderate impact to the business	Minor	External users have visibility of internal system(s) information, including system configurations	2
	System(s) or application(s), which if disrupted, have no impact to the business	None	External user(s) have limited to no visibility of internal assets	1
	Unknown	Unknown	Unknown	0

Figure 10. Anytime Fitness Score for Perimeter Mapping

Figure 11 indicates the company's risk rating based on the research results.

Company Risk Rating	
Score	**Risk**
7 – 9	High
4 – 6	Medium
1 – 3	Low
0	Unknown

Figure 11. Anytime Fitness Risk Rating

5.2. Comcast Corporation

As per the VCDB, the organization has five publicly reported incidents. All five incidents resulted in a breach of customer data totaling more than 30 million impacted individuals. Figure 12 indicates the criteria for security incidents and the company's average risk score (highlighted).

	Security Incidents			
	Categories			
	Incident Type	**Incident Impact**	**Incident Volume**	**Score**
Criteria	Information breach or long-term outage to business operations	Catastrophic	Multiple security incidents	3
	Temporary disruption to business processes or services	Moderate	One security incident	2
	Local, isolated event	Insignificant	No security incidents	1
	Unknown	Unknown	Unknown	0

Figure 12. Comcast Corporation Score for Security Incidents

Comcast Corporation has 1,002 publicly identified assets based on the results from perimeter mapping. SANS ISC did not contain any intelligence related to those assets. Research through Google and other search engines did identify intelligence indicating state-sponsored threat actor(s) targeted Internet Service Providers such as Comcast (US-CERT, 2018). Figure 13 includes the criteria for threat intelligence and the company's average risk score (highlighted).

	Threat Intelligence			
	Categories			
	Threat Motivation	**Threat Capabilities**	**Threat Frequency**	**Score**
Criteria	Threat actor(s) conduct attack(s) that require extended planning and execution, such as espionage and ideology-based attack(s)	Threat actor(s) exhibit advanced techniques and resources common to state-sponsored groups	Attack(s) are carried out over extended, targeted campaigns	3
	Threat actor(s) are focused on short-term results, such as monetary gain or revenge	Threat actor(s) demonstrate the ability to create custom exploits as necessary	Attack(s) occur semi-frequently but do not indicate coordinated efforts	2
	Threat actor(s) are not motivated by any specific goal or target	Threat actor(s) rely on weak security controls or techniques with inconsistent success	Attack(s) are isolated to random windows of opportunity and follow no patterns or trends	1
	Unknown	Unknown	Unknown	0

Figure 13. Comcast Corporation Score for Threat Intelligence

Recon-ng did identify systems with private IP addresses among the discovered assets as per the RFC 1918 standard. Shodan did not provide any results indicating internal assets performed sensitive processes or contained vulnerabilities, which would have allowed further visibility or access. Figure 14 includes the criteria for perimeter mapping and the company's average risk score (highlighted).

	Perimeter Mapping			
	Categories			
	Asset Function	**Asset Valuation**	**Asset Exposure**	**Score**
Criteria	System(s) or application(s) that stores sensitive information or performs critical business functions	Major	External users can directly access internal system(s)	3
	System(s) or application(s), which if disrupted, may cause minimal to moderate impact to the business	Minor	External users have visibility of internal system(s) information, including system configurations	2
	System(s) or application(s), which if disrupted, have no impact to the business	None	External user(s) have limited to no visibility of internal assets	1
	Unknown	Unknown	Unknown	0

Figure 14. Comcast Corporation Score for Perimeter Mapping

Figure 15 indicates the company's risk rating based on the research results.

Company Risk Rating	
Score	**Risk**
7 – 9	High
4 – 6	Medium
1 – 3	Low
0	Unknown

Figure 15. Comcast Corporation Risk Rating

5.3. Peachtree Neurological Clinic, PC

The VCDB contained two security incidents for this organization. The company reported a ransomware attack in 2017, which led investigators to discover a 15-month long breach starting in 2016 (Davis, 2017). Although details were limited, the company disclosed the threat actor may have had access to sensitive customer data. Figure 16 indicates the criteria for security incidents and the company's average risk score (highlighted).

	Security Incidents			
	Categories			
	Incident Type	**Incident Impact**	**Incident Volume**	**Score**
Criteria	Information breach or long-term outage to business operations	Catastrophic	Multiple security incidents	3
	Temporary disruption to business processes or services	Moderate	One security incident	2
	Local, isolated event	Insignificant	No security incidents	1
	Unknown	Unknown	Unknown	0

Figure 16. Peachtree Neurological Clinic, PC Score for Security Incidents

From perimeter mapping, the organization maintains one publicly identifiable asset: their website, www[.]peachtreeneurological[.]com. Threat intelligence did not provide additional information about this domain or company, except details from the previously mentioned incidents. Figure 17 includes the criteria for threat intelligence and the company's average risk score (highlighted).

	Threat Intelligence			
	Categories			
	Threat Motivation	**Threat Capabilities**	**Threat Frequency**	**Score**
Criteria	Threat actor(s) conduct attack(s) that require extended planning and execution, such as espionage and ideology-based attack(s)	Threat actor(s) exhibit advanced techniques and resources common to state-sponsored groups	Attack(s) are carried out over extended, targeted campaigns	3
	Threat actor(s) are focused on short-term results, such as monetary gain or revenge	Threat actor(s) demonstrate the ability to create custom exploits as necessary	Attack(s) occur semi-frequently but do not indicate coordinated efforts	2
	Threat actor(s) are not motivated by any specific goal or target	Threat actor(s) rely on weak security controls or techniques with inconsistent success	Attack(s) are isolated to random windows of opportunity and follow no patterns or trends	1
	Unknown	Unknown	Unknown	0

Figure 17. Peachtree Neurological Clinic, PC for Threat Intelligence

As mentioned, the organization does not have a significant public footprint. Furthermore, Shodan did not identify any vulnerabilities of their website. Figure 18 includes the criteria for perimeter mapping and the company's average risk score (highlighted).

	Perimeter Mapping			
	Categories			
	Asset Function	**Asset Valuation**	**Asset Exposure**	**Score**
Criteria	System(s) or application(s) that stores sensitive information or performs critical business functions	Major	External users can directly access internal system(s)	3
	System(s) or application(s), which if disrupted, may cause minimal to moderate impact to the business	Minor	External users have visibility of internal system(s) information, including system configurations	2
	System(s) or application(s), which if disrupted, have no impact to the business	None	External user(s) have limited to no visibility of internal assets	1
	Unknown	Unknown	Unknown	0

Figure 18. Peachtree Neurological Clinic, PC for Perimeter Mapping

Figure 19 indicates the company's risk rating based on the research results.

Company Risk Rating	
Score	**Risk**
7 – 9	High
4 – 6	Medium
1 – 3	Low
0	Unknown

Figure 19. Peachtree Neurological Clinic, PC Risk Rating

5.4. Seidl's Party Supplies & Rental

An unknown individual physically robbed the company in 2017, and stole customer credit card information and their payment processing machine (ABC 10News, 2017). Further investigation did not identify any other incidents. Figure 20 indicates the criteria for security incidents and the company's average risk score (highlighted).

	Security Incidents			
	Categories			
	Incident Type	**Incident Impact**	**Incident Volume**	**Score**
Criteria	Information breach or long-term outage to business operations	Catastrophic	Multiple security incidents	3
	Temporary disruption to business processes or services	Moderate	One security incident	2
	Local, isolated event	Insignificant	No security incidents	1
	Unknown	Unknown	Unknown	0

Figure 20. Seidl's Party Supplies & Rental Score for Security Incidents

Due to the size of the business and their small public footprint, the isolated, physical incident reported in the VCDB provided the only threat intelligence. Figure 21 includes the criteria for threat intelligence and the company's average risk score (highlighted).

	Threat Intelligence			
	Categories			
	Threat Motivation	**Threat Capabilities**	**Threat Frequency**	**Score**
Criteria	Threat actor(s) conduct attack(s) that require extended planning and execution, such as espionage and ideology-based attack(s)	Threat actor(s) exhibit advanced techniques and resources common to state-sponsored groups	Attack(s) are carried out over extended, targeted campaigns	3
	Threat actor(s) are focused on short-term results, such as monetary gain or revenge	Threat actor(s) demonstrate the ability to create custom exploits as necessary	Attack(s) occur semi-frequently but do not indicate coordinated efforts	2
	Threat actor(s) are not motivated by any specific goal or target	Threat actor(s) rely on weak security controls or techniques with inconsistent success	Attack(s) are isolated to random windows of opportunity and follow no patterns or trends	1
	Unknown	Unknown	Unknown	0

Figure 21. Seidl's Party Supplies & Rental Score for Threat Intelligence

The company maintains a single website, www[.]seidlspartyrentals[.]com, which only provides information about the company and is not used to conduct business. Figure 22 includes the criteria for perimeter mapping and the company's average risk score (highlighted).

	Perimeter Mapping			
	Categories			
	Asset Function	**Asset Valuation**	**Asset Exposure**	**Score**
Criteria	System(s) or application(s) that stores sensitive information or performs critical business functions	Major	External users can directly access internal system(s)	3
	System(s) or application(s), which if disrupted, may cause minimal to moderate impact to the business	Minor	External users have visibility of internal system(s) information, including system configurations	2
	System(s) or application(s), which if disrupted, have no impact to the business	None	External user(s) have limited to no visibility of internal assets	1
	Unknown	Unknown	Unknown	0

Figure 22. Seidl's Party Supplies & Rental Score for Perimeter Mapping

Figure 23 indicates the company's risk rating based on the research results.

Company Risk Rating	
Score	**Risk**
7 – 9	High
4 – 6	Medium
1 – 3	Low
0	Unknown

Figure 23. Seidl's Party Supplies & Rental Risk Rating

6. Summary Findings

6.1. Analysis and Recommendations

Acquiring companies may determine a target company with a specific risk rating poses too significant a risk to proceed with an M&A deal. However, other organizations could opt to proceed with the M&A deal and use the collected information to justify future remediation activities. For example, Peachtree Neurological Clinic discovered a breach approximately one year after it initially occurred, which could indicate insufficient monitoring controls of sensitive data. Acquiring companies may elect to audit their data management policies, implement a Data Loss Protection tool, or perform a data mapping exercise to understand how and where information is processed and stored. Although a company's risk rating may not be sufficient to singularly affect the outcome of a future deal, acquiring companies can use the information as a baseline for future projects and security controls.

The study used the tools and data sources previously mentioned for each test case. This study's scope focused on providing a standardized approach and did not seek to identify the most viable tool available. However, researchers should compare alternative options in order to increase confidence in their results. For example, research into Seidl's Party Supplies & Rental revealed few details about the organization, likely due to their market size and a lack of technology dependency. Although fewer results do not indicate a lack of evidence, acquiring organizations using this framework should exhaust all reliable solutions.

The framework requires subjective analysis in some areas. Specifically, the researcher must define Incident Impact and Asset Valuation. The framework did not define these criteria more strictly because acquiring companies are likely to diverge on standard or generalized definitions. For that reason, a company's risk rating cannot be publicly shared or distributed for general consumption.

6.2. Additional Considerations/Future Research

In addition to the suggestions provided by this study, future researchers may find valuable information about a potential M&A candidate through other, less-established means and methodologies.

Third-party vendors conducting business with a company may publicly disclose the business relationship through news statements or a public customer list on their external website. With the additional context of the products and services provided by a third party, acquiring companies can infer information about processes and technologies, which reveal potential vulnerabilities and undisclosed security incidents. SolarWinds maintained a public list of customers on their website for several days after the SUNBURST incident was announced (Jankowicz & Davis, 2020). Although the company took steps to conceal their customers' privacy, SolarWinds potentially increased their customers' exposure to threat actors by publicizing their use of vulnerable software.

Current and former employees of a target company can also unintentionally reveal information about software and hardware used by companies. LinkedIn, a popular social media platform used for social networking, allows users to share information about their skills and responsibilities. By searching for employees of a specific company, researchers may find software and hardware used by an employee while under their employment. When corroborated through additional open-source intelligence, acquiring companies could use this knowledge to gain information about a target's internal environment.

7. Conclusion

This study identified pertinent information, examined tools, and provided a new framework to assess the risk of a potential M&A target company. The framework allows acquiring companies to create a risk score, which can be added to other analyses to understand the strengths and weaknesses of multiple target companies, independent of any logical boundaries such as industry or customer base. Furthermore, acquiring companies can use the collected information and referenced tools as a baseline to help onboard a company after the acquisition phase. Although this study includes Information

Security concepts and methodologies, this framework can help communicate an organization's risk to stakeholders across all vertical industries and sectors.

References

ABC 10News. (2017, October 27). *Ramona business robbed, customer data stolen*. https://www.10news.com/news/ramona-business-robbed-customer-credit-card-information-stolen

Bromiley, M. (2019, December 8). *Threat hunting with consistency*. SANS Institute Reading Room. https://www.sans.org/reading-room/whitepapers/analyst/threat-hunting-consistency-39315

Chappell, B. (2018, September 27). *Uber pays $148 million over yearlong cover-up of data breach*. NPR. https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach

Davis, J. (2017, July 19). *Atlanta clinic finds 15-month breach during investigation on separate ransomware attack*. Healthcare IT News. https://www.healthcareitnews.com/news/atlanta-clinic-finds-15-month-breach-during-investigation-separate-ransomware-attack

Harroch, R., Martin, J., & Smith, R. V. (2018, November 11). *Data privacy and cybersecurity issues in mergers and acquisitions*. Forbes. https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/?sh=3d13c2a472ba

Hartman, A. (2002). *Security considerations in the merger/acquisition process*. SANS Institute Reading Room. https://www.sans.org/reading-room/whitepapers/casestudies/security-considerations-merger-acquisition-process-667

Haspeslagh, P. C., & Jemison, D. B. (1991). *Managing acquisitions: Creating value through corporate renewal*. Free Press.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Institute for Mergers, Acquisitions and Alliances. (n.d.). *M&A statistics*. Retrieved December 15, 2020, from https://imaa-institute.org/mergers-and-acquisitions-statistics/

Jankowicz, M., & Davis, C. (2020, December 15). *These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia*. Business Insider. https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12

Jelen, S. (2019, June 6). *Find vulnerabilities before they become yours: Cybersecurity with mergers and acquisitions*. SecurityTrails. https://securitytrails.com/blog/cybersecurity-mergers-acquisitions

Jemison, D. B., & Sitkin, S. B. (1986, March). Acquisitions: The process can be a problem. *Harvard Business Review*. https://hbr.org/1986/03/acquisitions-the-process-can-be-a-problem

Lidome, P. (2020, October 26). *The SANS guide to evaluating attack surface management*. SANS Institute Reading Room. https://www.sans.org/reading-room/whitepapers/analyst/guide-evaluating-attack-surface-management-39905

Maltego. (n.d.). *Downloads*. Retrieved April 6, 2021, from https://www.maltego.com/downloads/

Mapgaonkar, D., & Perinkolam, A. (2016). *Don't drop the ball identify and reduce cyber risks during M&A*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-ma-dont-drop-the-ball-Identify-and-reduce-cyber-risks-during-m-and-a.pdf

NAICS Association. (n.d.-a). *History of the NAICS code*. Retrieved February 2, 2021, from https://www.naics.com/history-naics-code/

NAICS Association. (n.d.-b). *Market research*. Retrieved February 15, 2021, from https://www.naics.com/market-research/

Offensive Security. (n.d.). *Recon-ng package description*. Kali Linux Tools. https://tools.kali.org/information-gathering/recon-ng

Olyaei, S. (2018, April 30). *Cybersecurity is critical to the M&A due diligence process* (G00259444). Gartner. https://www.gartner.com/en/documents/3873604

SANS Institute. (n.d.-a). *About us*. Internet Storm Center. Retrieved February 18, 2021, from https://isc.sans.edu/about.html

SANS Institute. (n.d.-b). *Our risk score*. Internet Storm Center. Retrieved February 12, 2021, from https://isc.sans.edu/risk.html

Shodan. (2020, November 2). *What is Shodan?* Retrieved February 21, 2021, from https://help.shodan.io/the-basics/what-is-shodan

SolarWinds. (2021, January 29). *Security advisory*. Retrieved February 18, 2021, from https://www.solarwinds.com/sa-overview/securityadvisory

US-CERT. (2018). *Russian state-sponsored cyber actors targeting network infrastructure devices* (TA18-106A). CISA. https://us-cert.cisa.gov/ncas/alerts/TA18-106A?utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_british_parliament_moves_toward_a_more_coordinated_investigation&utm_term=2019-03-16

U.S. Small Business Administration. (n.d.). *Size standards*. Retrieved February 20, 2021, from https://www.sba.gov/federal-contracting/contracting-guide/size-standards

Verizon RISK. (2013, September 12). *Vz-risk/VCDB*. GitHub. Retrieved February 20, 2021, from https://github.com/vz-risk/VCDB/wiki

Verizon RISK. (2014, December 4). *Vz-risk/VCDB*. GitHub. Retrieved February 20, 2021, from https://github.com/vz-risk/VCDB

Verizon. (2017, July 21). Announcing veriscommunity.net. https://enterprise.verizon.com/resources/articles/announcing-veriscommunity/

Verizon. (2020). *2020 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Wheeler, E. (2011). *Security risk management*. Elsevier. https://doi.org/10.1016/B978-1-59749-615-5.00018-9

Wright, J. (2015, December 8). *Getting the most out of Shodan searches*. SANS. Retrieved February 21, 2021, from https://www.sans.org/blog/getting-the-most-out-of-shodan-searches/

Appendix

Maltego System and Network Requirements (Maltego, n.d.)

- Java 8 64 bit (minimum) / Java 11 64 bit (recommended)
- 4GB of RAM (required) / 16 GB (recommended)
- 4 GB of disk space
- Client access to the Internet:
    - Outbound Ports: 80, 443, 8081; Port 5222 to join shared graphs on the public server
    - Additional ports as necessary for third-party transform vendors

Templates for Risk Profiling Framework

	Security Incidents			
	Categories			
	Incident Type	**Incident Impact**	**Incident Volume**	**Score**
Criteria	Information breach or long-term outage to business operations	Catastrophic	Multiple security incidents	3
	Temporary disruption to business processes or services	Moderate	One security incident	2
	Local, isolated event	Insignificant	No security incidents	1
	Unknown	Unknown	Unknown	0

	Threat Intelligence			
	Categories			
	Threat Motivation	**Threat Capabilities**	**Threat Frequency**	**Score**
Criteria	Threat actor(s) conduct attack(s) that require extended planning and execution, such as espionage and ideology-based attack(s)	Threat actor(s) exhibit advanced techniques and resources common to state-sponsored groups	Attack(s) are carried out over extended, targeted campaigns	3
	Threat actor(s) are focused on short-term results, such as monetary gain or revenge	Threat actor(s) demonstrate the ability to create custom exploits as necessary	Attack(s) occur semi-frequently but do not indicate coordinated efforts	2
	Threat actor(s) are not motivated by any specific goal or target	Threat actor(s) rely on weak security controls or techniques with inconsistent success	Attack(s) are isolated to random windows of opportunity and follow no patterns or trends	1
	Unknown	Unknown	Unknown	0

	Perimeter Mapping			
	Categories			
	Asset Function	**Asset Valuation**	**Asset Exposure**	**Score**
Criteria	System(s) or application(s) that stores sensitive information or performs critical business functions	Major	External users can directly access internal system(s)	3
	System(s) or application(s), which if disrupted, may cause minimal to moderate impact to the business	Minor	External users have visibility of internal system(s) information, including system configurations	2
	System(s) or application(s), which if disrupted, have no impact to the business	None	External user(s) have limited to no visibility of internal assets	1
	Unknown	Unknown	Unknown	0

Company Risk Rating	
Score	**Risk**
7 – 9	High
4 – 6	Medium
1 – 3	Low
0	Unknown

Recon-ng Commands

Recon-ng commands executed to perform analysis against the 4 test cases:

workspaces create <workspace>

marketplace refresh

marketplace install <module>

modules load <module>

keys add <name> <value>

modules load <module>

VCDB and Recon-ng Results

The VCDB and Recon-ng results for the four test cases can be found at https://github.com/ltwhit/cyberriskprofile_ma.