electronics

MDPI

Article

Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports

Omer F. Keskin, Kevin Matthe Caramancion, Irem Tatar, Owais Raza and Unal Tatar *

College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, State University of New York, Albany, NY 12203, USA; okeskin@albany.edu (O.F.K.); kcaramancion@albany.edu (K.M.C.); itatar@albany.edu (I.T.); oraza@albany.edu (O.R.)
* Correspondence: utatar@albany.edu

Abstract: Cybersecurity is a concern for organizations in this era. However, strengthening the security of an organization's internal network may not be sufficient since modern organizations depend on third parties, and these dependencies may open new attack paths to cybercriminals. Cyber Third-Party Risk Management (C-TPRM) is a relatively new concept in the business world. All vendors or partners possess a potential security vulnerability and threat. Even if an organization has the best cybersecurity practice, its data, customers, and reputation may be at risk because of a third party. Organizations seek effective and efficient methods to assess their partners' cybersecurity risks. In addition to intrusive methods to assess an organization's cybersecurity risks, such as penetration testing, non-intrusive methods are emerging to conduct C-TPRM more easily by synthesizing the publicly available information without requiring any involvement of the subject organization. In this study, the existing methods for C-TPRM built by different companies are presented and compared to discover the commonly used indicators and criteria for the assessments. Additionally, the results of different methods assessing the cybersecurity risks of a specific organization were compared to examine reliability and consistency. The results showed that even if there is a similarity among the results, the provided security scores do not entirely converge.

Keywords: cyber risk; third-party risk; supply chain risk; vendor risk; risk scoring; cyber insurance

Citation: Keskin, O.F.; Caramancion, K.M.; Tatar, I.; Raza, O.; Tatar, U. Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics* **2021**, *10*, 1168. https://doi.org/10.3390/electronics10101168

Academic Editors: Changhoon Lee, Yu Chen and Jake (Jaeik) Cho

Received: 20 January 2021
Accepted: 4 May 2021
Published: 13 May 2021

1. Introduction

Supply chains are crucial for the viability of today's global organizations. With the high degree of dependencies among organizations, no business processes (i.e., missions) can succeed without receiving the products or services from third-party organizations [1]. Information and communication technologies (ICT) enable organizations to operate as a part of this highly interconnected supply chain; however, they also pose the organizations to cyber risks due to their vulnerabilities [2].

Vendors allow a company to acquire specialist skills and knowledge that can significantly differentiate the value of an organization's end-products and services. However, receiving services or products from vendors also increases the risks posed by these vendors' vulnerabilities. Third-Party Risk Management (TPRM) is the process used by companies to monitor and manage interactions with all external parties, particularly their vendors. TPRM has been used for years by companies, but it is relatively new to the cyber domain. Data breaches have not only been caused by the compromises initiated within a company but also originated at a business partner, supplier, or other third-party organizations. Such risks are considered part of the Cyber Third-Party Risk Management (C-TPRM), and this term can be used interchangeably with vendor cyber risks and cyber supply chain risks. With an effective C-TPRM, a company can mitigate such vulnerabilities to avoid risks caused by its dependencies.

The efficiency of supply chains requires organizations to share information and increase interdependencies among their information technology (IT) networks, which signifi-

cantly increases the attack surface of an organization [3]. According to a report by Resilinc, the likelihood of a manufacturing organization experiencing a supply chain disruption in 24 months is more than 98% [4]. Another report by PwC notes that in 2014, current service providers and contractors were responsible for 23% of all cyber breaches, while past partners were responsible for 45% [5]. Based on a survey report by Ponemon Institute [6], 56% of organizations have experienced a data breach, and 75% of organizations have experienced a cyber incident caused by their third-party vendors. While the average number of third parties with access to a given organization's sensitive data is 471, merely one-fifth of the organizations know if their suppliers share their data with any other supplier. Third-party cyber risks are on the rise, while regulations and mitigation techniques against third-party cyber risks are still in the early stages [7].

The purpose of this study is to examine the C-TPRM solutions available in the market and compare their results (i.e., third-party risk scores) to assess the reliability and consistency of these risk scores. In this study, we are addressing the following research questions:

1. What methods are currently used in cyber third-party risk management?
2. How reliable do different scoring tools calculate the third-party risk scores?

The paper is organized as follows: Section 2 presents the previous work on this topic, including the existing risk analysis methods. Section 3 discusses and analyzes some of the most significant cyberattacks regarding C-TPRM. Section 4 elaborates the methodology of the study. Section 5 provides insights on different approaches for quantifying third-party cyber risks by different companies, the common indicators used for quantification, and a benchmarking of results by different C-TPRM approaches for a specific higher education institute. Section 6 presents the results of the analysis. Section 7 discusses the findings of the study and provides directions for future research. Section 8 concludes the paper by discussing its contributions.

2. Previous Work

The literature review section comprises a summary of relevant works in the literature summarizing the methods for calculating the third-party cyber risk.

2.1. Risk Management

Risk is defined by Kaplan and Garrick [8] as a function of probability and consequences of a loss event. This concept applies to cybersecurity risks. Various methods exist in the literature to quantify the cybersecurity risks that can be chosen or adapted based on the characteristics of the organization under focus and the threat landscape [9]. Threats and vulnerabilities are commonly used to estimate the risks [10]. A threat is defined as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" [11]. A vulnerability is defined as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [11]. Several risk assessment methods exist, including EBIOS, MEHARI, OCTAVE, IT-Grundschutz, MAGERIT, CRAMM, HTRA, NIST SP 800–30, NIST SP 800–37, NIST SP 800–39, RiskSafe Assessment, and CORAS [12,13]. The methods and frameworks are either or both qualitative and quantitative [14,15]. The criteria to select the correct model include validity, compliance, cost, and usefulness. Most of these methods only focus on the organization's inherent risks instead of considering the risks posed by the connections or dependencies with the organization's vendors [16].

Organizations utilize various types of methods to assess cybersecurity risks: qualitative, quantitative, and hybrid risk assessment. Qualitative risk assessment is commonly used since it is relatively easy and faster to conduct. Risk events are identified, and for each risk, event likelihood and consequences are estimated based on a scale, typically as low, medium, and high. Finally, they are visualized on a risk matrix (heat map) to prioritize

and determine mitigation actions. However, it is subjective, and the complexity of larger organizations requires objective and quantified methods. Quantitative risk assessment can be conducted in a tailored way for each organization based on the characteristics of the organization's network. Risk managers, system owners, and system administrators need to employ models to assess cyber risks. Hybrid methods combining qualitative and quantitative methods can also be utilized. Cyber risk management frameworks are provided by organizations such as the National Institute of Standards and Technology (NIST) and the International Standards Organization (ISO). These frameworks [11,17–21] provide detailed steps for risk management, including lists of security controls to mitigate the cyber risks. Such frameworks can be adopted by organizations and tailored to assess cybersecurity risks.

Organizations utilize risk management frameworks as a guide to tailor the risk management best practices to the characteristics of their sector and organization. Multiple frameworks have been published [22]. Among others, frameworks by the NIST, ISO, and MITRE are widely used by governmental and private organizations throughout the USA and the world. Several factors affect the decision on selecting a framework. First, The ISO/IEC 27000 series [20] is an international standard that provides guidance on establishing a risk management-based information security management system. With its broad scope, ISO/IEC 27000 can be adopted by any organization regardless of size and sector. On the other hand, NIST's cyber risk management publications integrate security and risk management activities into the system development life cycle. While ISO/IEC 27000 has an international audience and is adopted worldwide, the NIST guidelines are dominant in the United States and applied mainly by federal agencies, government contractors, and critical infrastructure operators. Frameworks developed by MITRE usually focus on vulnerability and threat management that is an integral part of risk management.

After selecting a risk management framework, an organization needs to adopt it based on its characteristics. As an example, adopting NIST's risk management framework is succinctly explained in this paragraph. Three risk management documents of NIST (i.e., NIST SP 800–39, 30, and 37) enables organizations to integrate cyber risk management into enterprise risk management by providing multi-tiered risk management by examining risk at the information systems level, business process level, and organizational level instead of considering cyber risk as a silo. NIST SP 800–30 [19] defines cyber risk as "a function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." In compliance with this definition, NIST SP 800–39 [17] and NIST SP 800–37 r.2 [18] explain how to integrate risk management process throughout the organization by addressing cyber risks at three levels, from tactical to strategic order: information systems level, mission/business process level, and organizational level. NIST SP 800–39 [17] also discusses the effects of organizational culture on risk management, which is an essential element of ERM.

2.2. Supply Chain Cybersecurity

Trust among the organizations of a supply chain plays an integral role [23]. Relationships based on trust increase cooperation over time, resulting in better responsiveness. Instrumental in a continuous exchange of materials, information, and knowledge, supply chains have evolved into complex and interdependent networks. Alongside the risks stemming from complexity and interdependencies, extensive use of information and communication technologies (ICT) has posed cyber risks to supply chains. Concerns regarding data privacy also increased along with emerging cyber risks. Trust among supply chain entities in the era of connectivity evolved since success in supply chain operations does not ensure the cybersecurity of a network [24–26]. Mitigating cyber risks and addressing privacy concerns has become an essential step to ensure trust among supply chain entities. Researchers in this field develop new models to address such issues to contribute to building trust among partner organizations [25,27].

The integration of ICT with supply chain size and technology heterogeneity has increased significantly. This requires organizations to deal with a new set of problems that have not been traditionally existed. Ensuring confidentiality, integrity, and availability of the data and services provided by the ICT network is a challenging task that organizations need to undertake. While increased connectivity not only helps operations but also opens new doors to the attackers, every single software and hardware component added to the network is a potential vulnerability that can be exploited by adversaries. For example, the introduction of the Internet of Things (IoT) increases the ability to gather much more information about the process; however, not all IoT designers prioritize cybersecurity [28]. This insecurity introduces new challenges to the network administrators.

Emerging technological developments try to address some of the issues encountered by supply chain operators. Blockchain technology is an emergent field regarding ICT networks. The immutability of blockchain technology and smart contracts brings the ability to provide traceability sought by industries such as food and pharmaceuticals. Even though blockchain technology can be promising to address some of the issues, there are still many risks regarding the cybersecurity of the supply chain [25,27–35].

2.3. Supply Chain Cyber Risk Analysis

Cyber supply chain risk management is a relatively new field that combines expertise in cybersecurity, supply chain management, and enterprise risk management [36]. Early discussions of the effects of cyber attacks on the supply chain listed and explained different attack types [37]. Boyson et al. [38] developed a cyber supply chain assurance reference model. Then, Storch [39] developed a risk-based software integrity management approach. Supply chain risk management literature mainly focuses on risks related to product flow and supplier selection. Some literature also considers the financial aspect by adding cash flow risks to the product flow risks.

Risk assessment is commonly conducted by estimating the likelihood and consequences (impact) of cyber incidents. For the likelihood estimation component of the cyber risk analysis, identifying and scoring the organization's vulnerabilities is crucial. Intrusive and non-intrusive methods are two of the main approaches for vulnerability analysis and likelihood estimation. Intrusive cyber risk assessment methods are conducted by direct interaction with the subject organization's network and require their actions. These methods include network vulnerability scanning, reviewing logs, audits, and penetration testing. On the other hand, non-intrusive methods are used to assess an organization without any involvement of the subject. It includes techniques such as checking the subject's Web site for outdated certificates, looking up IP addresses of servers of the subject at the botnet registers, and searching the dark Web for any breached confidential data belonging to the subject organization. A third method includes conducting a survey-like approach where a checklist of security controls would be asked from the subject organization to be filled out to evaluate the security level without conducting any technical analysis. These three approaches differ in their depth and convenience. Only the non-intrusive methods are in the scope of this study.

MITRE's Supply Chain Attacks and Resiliency Mitigations report [40] demonstrates how cyber threats can pose risks at any phase of the acquisition lifecycle (i.e., material solution analysis, technology development, engineering, manufacturing development, production, deployment, operations, and support). The NIST started the Cyber Supply Chain Risk Management (C-SCRM) program in 2008 to "Develop a multi-pronged approach for global supply chain risk management" by working with diverse stakeholders from "government, industry, and academia to identify and evaluate effective technologies, tools, techniques, practices, and standards useful in securing the cyber supply chain." One of the significant outputs of the program is NIST Special Publication 800–161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations [41].

McDaniel et al. [42] identified challenges and problems with the cyber supply chain and developed the Trustworthy Supplier Framework to constitute guidance to minimize

supply chain security incidents. The purpose of this framework is to assure that the suppliers along the supply chain are trustworthy, and they will make sure that no modification, whether intentional or unintentional, will occur on the ICT products. The framework is still being improved; the effectiveness or cost benefits of using this framework have not been tested yet.

All of these efforts establish a set of principles for a secure and resilient supply chain. However, organizations still require a practical approach to assess the cyber risks posed by their partners in the supply chain. This study will benchmark the existing approaches of non-intrusive third-party cyber risk management in order to investigate the consistency of the existing approaches.

3. Case Analysis of Infamous Cyber Attacks Regarding C-TPRM

This section discusses how third-party risks can cause cyber incidents by analyzing five important cyber attack cases: Target, Home Depot, Office of Personnel Management, RSA Security, and SolarWinds.

3.1. Target

Target data breach is one of the most significant examples of third-party cyber risks hidden in supply chains. In late 2013, the credit and debit card information of more than 40 million customers along with non-financial details of some 70 million customers were stolen from Target. Merely reissuing the customer cards cost the banks more than 200 million dollars [43]. Target was also affected as they had to pay $18.5 million in a class-action lawsuit against them, excluding the cost of lawyer fees, as it took about four years before a settlement was reached [44].

Although Target has been compliant with legal and industry standards, not all companies within their supply chain had a sufficient level of cybersecurity [45]. Attackers used this opportunity to conduct a successful phishing attack and steal network credentials from one of the vendors of Target, Fazio Mechanical Services. This small company sells heating, ventilation, and air-conditioning systems to Target. Then, attackers set foot on Target's network via the vendor portal that was meant to be used by the vendors for external billing, contract, and project management purposes. Attackers moved on to deploy a custom software called BlackPOS on the point-of-sale systems. The malware had the ability to scrap unencrypted, plain text data, including PIN codes, within the memory of the POS terminal before they were encrypted. Having completed developing the malware, the attackers fully deployed it on the POS machines. The attackers also installed another malware within the Target network to exfiltrate the data to drop locations outside the network. The attackers were comfortable enough to test and update the malware multiple times to improve its operation. Even though the intrusion triggered alerts on Target's intrusion detection systems and antivirus software, the security team did not react against the suspicious activity. The malicious software stored and exfiltrated data, including details of all cards swiped, within a couple of weeks to the drop locations [46]. The attackers later retrieved the stolen information and sold it on the black market. After the Department of Justice informed Target about the attack, the company publicly announced the breach.

After the breach, many analysts concluded that Target had a chance to stop the breach from happening and limit the number of customers affected. Though not entirely scientific, a counterfactual approach might help us grasp the matter more clearly: if the computers of Fazio, Target's vendor, had had antivirus software, authentication stealing malware would have triggered the alert and prevented the attack from happening. Additionally, Target should have segmented their networks to ensure that Fazio and other third parties did not have access to their payment systems. Moreover, Target's security team could have paid attention to the alerts they received from the intrusion detection system regarding the escape routes the attackers planned to use to exfiltrate data from Target's network to prevent the data breach [46].

However, Target did learn from this attack and has implemented some new security policies to prevent future attacks. One is to keep updated anti-intrusion software and hire a capable IT team that will monitor the network for any possible malicious activity. Another additional security policy is keeping their third-party partners at a high standard on their security controls [45].

3.2. Home Depot

On 14 September 2014, Home Depot, the largest home improvement retailer in the United States, experienced a massive data breach. Hackers were able to steal more than 50 million credit card numbers from Home Depot customers, along with 53 million email addresses [47]. Home Depot had to pay at least $134.5 million in compensation to Visa, MasterCard, and various banks. Furthermore, more than 50 lawsuits were consolidated into two class-action suits on the consumer front, with the plaintiffs last year awarded $19 million [48]. Broken down, $13 million was to reimburse the losses of the victims and $6.5 million to provide them with identity protection services. In addition to those two big payouts, Home Depot had to pay affected financial institutions an additional $27 million, in total costing Home Depot $179 million.

Similar to the Target breach, the Home Depot breach resulted from stolen credentials from one of Home Depot's vendors (which has not been named). Criminals used a third-party vendor's username and password to enter the perimeter of Home Depot's network. However, these credentials were not the only items needed to hack into Home Depot's point-of-sale devices [49]. However, the simple credentials were only the small piece of the puzzle that allowed the hackers to acquire elevated rights that allowed them to navigate portions of Home Depot's network. Then, they exploited a zero-day vulnerability in Windows, which allowed the hackers to deploy a unique, custom-built malware on its self-checkout systems in the US and Canada. The malware was left undetected for five months between April and September 2014 [49]. Home Depot, similar to Target, blamed the supply chain for their breach; however, it was just another example of an inadequate network sequestration and vetting process.

Although the Target breach happened a year before this attack, this only showed that retailers need to tighten integration between inventory, teams, and systems. After the breach occurred, Home Depot did learn from the attack and implemented many countermeasures to prevent a future breach from happening. The first implementation is a continuous vulnerability and malicious movement scanning on the corporate network and POS network. The second implementation was to properly separate network connections between third-party vendors and the POS network. Last but not least, Home Depot has created proper monitoring capabilities and management techniques of third-party vendor identities and access.

3.3. Office of Personnel Management (OPM)

The United States Office of Personnel Management (OPM) serves as the leading human resources agency and personnel policy manager for the Federal Government. OPM directs employee management services, manages retirement, healthcare, and insurance benefits, merit-based and inclusive hiring into the civil service, and it provides a secure employment process [50].

On 15 April 2015, OPM became a victim of a massive data breach. The hackers were able to obtain millions of standard forms (SF) 86, which contain confidential information about family members, college roommates, foreign contacts, and psychological information [51]. Such information can be dangerous if in the wrong hands due to the extensive information these forms have on millions of federal workers. Information on more than 22 million former and current federal employees was affected.

The massive data breach on OPM was primarily the office's fault. That year, the agency was accused of having poor cyber hygiene and reduced visibility into the traffic on its systems. The agency also failed to prioritize cybersecurity; in the year of the hack, OPM

only allocated $7 million in funding their cybersecurity team [51]. This amount of funding placed them last on a list of other federal agencies. Due to the lack of funding and cyber practice, a third-party company working with OPM was breached by the hackers, who then were able to gain credentials to the OPM network [51]. Since this was not the first attack OPM experienced, this was the turning point for them to add some countermeasures to prevent such an attack from happening in the future again.

Two major countermeasures were created. The first is to build or contract an in-depth auditing program that would contain important information about the vulnerabilities OPM and its vendors possess. The second countermeasure is to deploy an agency-wide requirement of multi-factor authentication on end-user accounts.

3.4. RSA Security

RSA Security LLC, widely known as RSA, is an American computer and network security company with a focus on encryption and encryption standards. RSA is one of the major cybersecurity companies in the United States. Therefore, it was surprising when RSA came out to the public in 2011 that they had been victims of a cyber-attack. The hackers were able to extract information from RSA's IT systems. Specifically, compromised products include RSA's SecurID, which consists of a token, either hardware or software, which generates an authentication code at fixed intervals—for example, once a minute using a built-in clock and an encoded random key known as a seed [52]. Thus, with this information, the hackers could reduce the effectiveness of RSA's two-factor authentication. This type of information affects not only RSA but also any company that utilizes the two-factor authentication system of SecurID. Overall, the actual cost of the RSA data breach was confirmed to be around $66 million in direct and attributable costs [53]. It is important to note that this number does not include the cost RSA customers had to spend to reconstruct their two-factor authentication systems.

The massive data breach on RSA came to be from three steps. The first step was when the hacker sent "phishing" emails with the subject line "2011 Recruitment Plan" to two small groups of employees over two days [54]. Unfortunately, one of the employees clicked on the email and was directed toward an excel file. At first, the file did not seem to put RSA systems in danger, but the spreadsheet contained malware that used a previously unknown, i.e., "zero-day," flaw in Adobe's Flash software to install a backdoor [54]. This malware allowed the hacker to stay hidden from RSA detectors while stealing employee credentials to use those credentials to get into RSA's IT system. The third and last step was spiriting RSA files out of the company to a hacked machine at a hosting provider and then on to the hacker himself [54].

The RSA case shows that even the top computer and network company in the United States can be breached from having a vulnerability in one of their third-party products, which in this case was the Adobe software. Moreover, RSA being a third-party providing service to several organizations that depend on its compromised security products, many other organizations suffered losses regarding cyber third-party risks.

3.5. SolarWinds

The SolarWinds hack that occurred in 2020 is a supply chain attack that leveraged the software update infrastructure of SolarWinds to breach into more than 18,000 organizations' networks [55–58]. Microsoft's president identified this as the "largest and most sophisticated attack" that ever happened, even though the total impact of the attack is not yet known [59]. While analyzing its sophistication, it is estimated that more than a thousand engineers worked on the development and execution of the attack [59].

The attack is categorized as a supply chain attack because it leverages the software update infrastructure that is trusted by the victims. Attackers infiltrated thousands of organizations' networks by delivering the malware via compromised software update servers. SolarWinds Inc. is the developer of a set of software that is primarily used in network management, making them an excellent target for hackers who want to infil-

trate organizations' networks. The attackers use the *trust* established by SolarWinds to deliver the malware they developed and do their best to keep it hidden from cybersecurity practitioners of the victim organizations [55–57].

The success of the attack is also ensured by the efforts of the attackers to keep it hidden. Although the attack started in March 2020, it was detected in December 2020. Employees of a cybersecurity company [55,56] that is a victim of the hack identified a suspicious activity regarding multi-factor authentication. They discovered that an additional phone was registered for an employee without their knowledge [55,56,59]. Further investigations led to the discovery of the attack. Among thousands of victim organizations, only one could reveal the suspicious activity after months.

One reason the malicious codes of the software update are kept hidden is the delayed execution. Malware waited for 12 to 14 days before execution not to be detected by automated systems, such as malware sandboxes [55,56]. Large organizations employ such detection systems to pre-deploy software to check whether any malicious or unintended consequences emerge.

Another feature that kept the breach hidden is that the malware does not follow just one way of action [55,60]. Arbitrary actions of the malware make it more difficult for organizations to detect suspicious activity by comparing the findings of others. For different organizations, the attackers followed different strategies.

After the backdoor is opened to the attackers from the network of a victim, they had a view of the network and could further spread within the network. Organizations discovered that attackers targeted Microsoft Office 365 and Azure Cloud services that commonly included valuable information for the attackers [60]. They had the opportunity to escalate privileges to have even more power to manage the network and its components. They can spread to other connected third-party organizations [60]. Moreover, the impact is not only limited to information technology (IT) networks, but also the operational technology (OT) components are possibly at risk. OT includes systems such as HVAC, power distribution, perimeter sensors, and backup power systems [61].

The total impact of the breach is still not known. At least nine federal agencies and almost 100 private organizations are identified as victims of the attack, with numerous affected facilities for each organization [62]. The impact of the attack on each target organization ranges from minimal to a mystery [63].

This highly sophisticated attack showed that all the vendors we trust are vulnerable to such high-impact breaches. Organizations have numerous partners, and every single software used by an organization is a possible attack vector. The tradeoff for organizations about third-party selection is challenging. Partners with minimal cybersecurity practices are already at high risk. The high-end organizations are good at cybersecurity; however, they attract more attention from the attackers since exploiting them would open the back doors to all their client organizations [64]. SolarWinds breach is not the first of its kind, and with its high impact, it shows the high potential to new threat actors who would try to replicate and improve further [60].

4. Methodology

This study presents an exploratory analysis of C-TPRM solutions. In the previous section, we presented relevant concepts by discussing prior incidents regarding C-TPRM, providing a summary of existing cyber risk analysis methods.

To set the ground, in the next section, we discuss the solutions of different companies to quantify cyber third-party risks.

For the data collection and analysis step, we conduct a pilot study for a specific organization (a US-based higher education institute) with sample C-TPRM risk scores from four different companies that provide risk scoring services. Firstly, data are collected by gathering cyber risk reports for the target organization from each of the selected four companies. Then, quantitative and qualitative analyses are conducted for comparison of the results to check consistency and reliability. For the quantitative assessment, the risk

scores are normalized to compare by rescaling the overall risk score provided by each company to the range of 0–100. Qualitative analysis results of each report are compared manually. Findings of the analyses are reported in Section 6.3. Triangulation is conducted to improve the reliability of the research by getting two researchers to conduct the analyses separately and eventually compare the results.

5. Solution for Quantifying Cyber Third-Party Risks

The main idea behind the C-TPRM solutions is creating a risk score for every company similar to the personal or company credit scores. In the US, the credit score bureaus (e.g., Equifax, Trans Union, and Experian) use a standard calculation method utilizing several factors such as the number of accounts, types of accounts, used credit vs. available credit, length of credit history, and payment history. Usually, the overall credit scores from different bureaus for an individual are consistent and converge to a point. In this section, first, we examine the C-TPRM risk scoring solutions available in the market. Then, we discuss how these risk scores are calculated and what factors are employed in risk score calculation.

5.1. Companies and Their Products

Third-party cyber risk management has become very popular after the occurrence of significant incidents and the emergence of the cyber insurance sector. Cyber insurance providers need to quickly estimate the risk profile of a buyer for an effective and efficient underwriting process. Alongside the other factors, third-party (or vendor) risk scores have become essential tools on which the insurers rely. The demand for third-party cyber risk scores triggered the supply, and several companies started to respond to this demand. While there are over ten companies in the cyber risk scoring market, their products differ in scope, detail, and results. In this section, we examine leading cyber risk scoring companies.

5.1.1. BitSight

BitSight is a cybersecurity rating company that assesses companies, government agencies, and educational institutions. It is one of the first security rating companies. Since 2011, BitSight has assessed the cybersecurity of more than 200,000 companies [65]. BitSight assembles models that produce company ratings based on a scale that enables insurers to rule on businesses' ability to receive coverage. Similar to a credit score, BitSight's ratings range from 250 to 900 [66].

Although most features are comparable to the other companies that provide risk assessment, BitSight's strength is the proprietary method of data collection from which they exclusively own more than 120 sources, both commercial and licensed data that allows a more specialized insight of key risk vectors, many of which are unique to BitSight's assessment.

5.1.2. ComplyScore

ComplyScore is an information security and governance solutions provider that helps organizations comply with existing regulations to keep their systems secure. ComplyScore, as a solution, performs the integration of risks, compliance, and audit to eliminate redundancies, hence providing the streamlining of processes of organizations resulting in the highly effective management of compliance and risk [67].

ComplyScore documents the current status of vendors' information security practices and assesses the vendors' compliance with information security policies, including elements of applicable federal and state information security laws. However, it is not intended to be a certificate of compliance with these laws. Its purpose is to assess the strength of information security controls that vendors deploy to protect data and serve as a guide to conduct business with the vendors.

This assessment and the score produced are based on the vendor's self-declarations and documentation and not on-site audit. The report includes a description of the gaps

between vendors' information security programs and requirements, along with the recommended mitigation steps necessary to close the gap.

5.1.3. FICO

FICO is a well-recognized data analytics company that is focused on credit scoring services. FICO extends its scoring on Cyber Risk Quantification in the form of the FICO Cyber Risk Score, which indicates the likelihood that an organization will experience a cyber incident in the future [68]. The new Chartis Research report Cyber Risk Quantification Solutions, 2020, named FICO as a Cyber Risk Quantification Category Leader for the second consecutive year [69].

As a solution, FICO offered its Cyber Risk Score as an empirical score anchored on a Machine Learning model in determining the risk profile of an organization. The training sets used to build the model are collected non-intrusively and consist of historical data that depend on a comprehensive and diverse set of cybersecurity data signals, including past compromise. FICO utilizes a pre-defined set of indicators to assess the cybersecurity posture of IT systems, the infrastructures of networks, and the software and services of an organization.

The score can be used for self-assessment, vendor management, and for the purpose of external security audits such as cyber insurance profiling.

5.1.4. Interos

Interos was founded in 2005 to help customers understand risk in their multi-tier, global supply chains. Interos researched and assessed individual suppliers, providing clients complete supply chain maps, identifying risks, and alerting businesses for issues that require attention. Interos, unlike many other companies, does not provide a score and instead provides possible vulnerability indicators. The one thing that differs from most other companies is that their software is automated by Artificial Intelligence [70].

5.1.5. Recorded Future

Recorded Future is a private cybersecurity company established in 2009. The company focuses on the gathering, processing, examination, and dissemination of threat intelligence. Recorded Future uses proprietary machine learning and natural language processing algorithms to continuously collect and analyze data from the open Web, dark Web, and technical resources. The measurement results are presented in a range of 0–100 within a software-as-a-service portal [71].

5.1.6. RiskRecon

RiskRecon was founded in 2015 and has recently been acquired by MasterCard. RiskRecon's software as a service for C-TPRM enables enterprises to understand their vendors' cybersecurity performance based on continuous assessment of their systems against 39 security risk criteria. Assessments deliver security measurements, analytics, and analyst-level insights. RiskRecon uses publicly available data to build the organizations' security posture modeling to measure their overall security risk [72]. Similar to its competitors, the data gathered are fed into a combination of AI and data-driven technology to secure cyberspace, particularly toward industries.

RiskRecon provides risk prioritization based on risk event severity and asset value. The assessment outputs a score between 1 and 10. Contextualization of risk enables customers to effectively convert RiskRecon assessments into actionable items, providing capabilities for customers to engage their vendors on the problems that expose them to the most significant risks. RiskRecon's strength against its competitors, as they have claimed, is its high customization—i.e., the solutions provided are custom-tuned to match an organization's risk priorities.

5.1.7. NormShield

NormShield's cyber risk rating system enables enterprises to measure the probable financial loss from a cyber attack on a third-party, supplier, or business partner. They provide a score with a letter grade from A to F. NormShield's 3D Vendor Risk @ Scale platform consolidates three types of evaluations to provide more fidelity and streamline the process of assessing third-party risk. Combining cybersecurity ratings, compliance checks, and probable financial loss simplifies the complicated process of assessing a vast amount of third-party organizations. The NormShield provides precise, quantitative, and regularly updated data to assess and track the cyber risk posture of organizations [73].

5.1.8. Panorays

Panorays Ltd. is following many of the other companies in making their software automated in risk scoring. Panorays provides a score from 0 to 100. What differentiates Panorays from other companies is that they provide companies with questionnaires that companies give to third-party organizations before hiring them. Panorays' customized security surveys include only the inquiries that are relevant for each supplier. Panorays also helps companies ensure that they adhere to regulations and standards such as GDPR, CCPA, NYDFS, and SIG. This is accomplished with the security questionnaires. Suppliers can be verified whether they meet the expectations of regulatory measures as well as the internal policies of the customer company [74].

5.1.9. SecurityScorecard

SecurityScorecard is an information security rating company that evaluates the cybersecurity posture of corporate entities by conducting a scored analysis of cyber threat intelligence signals for third-party management and IT risk management. Color-coded letter grades from A to F and numerical scores from 0 to 100 are calculated based upon the identification of security vulnerabilities on corporate digital assets. Enterprises are scored on multiple categories of risk such as Web application security, network security, DNS health, public availability of breached data, IR reputation, mentions within underground hacker chatter, response time for patching, and susceptibility to social engineering attacks [75,76].

5.2. Common Indicators/Factors Used in Third-Party Risk Assessment

Reports are typically built from data revolving around the possible vulnerabilities in an organization's (internal) and the vendor's (external) system. Different C-TRPM analysis methods use distinct categories to create a model that generates a cyber risk score. The following are the general elements primarily included in the assessments:

5.2.1. Endpoint Behaviors

Assessment of endpoint behaviors involves looking for traces that give off cues on the status of the overall picture, information of security posture, and management of an organization, including but not limited to access authorizations, asset management, and audit logging—typically of end-devices.

Typical components scanned include browsers, operating systems, and antivirus software. This dimension involves assessing the health status of endpoint security by looking for evidence of endpoint compromise. Scans typically include workstations, servers, and laptops for any compromise, since these are usually the prerequisites of a medium-to-massive-sized data breach. As for the widely accepted scale and industry reference, the Real-time Blackhole Lists (RBLs) are published reporting on confirmed or suspected malicious activities (such as spamming or malware distribution) originating from the endpoints of a network maintained by the broader security community. The underlying argument is that the communication in the protocol stack initiates and ends on these hosts, highlighting the importance of securing these through Intrusion Detection/Prevention Systems [77].

5.2.2. Network Misconfigurations

Assessment of network misconfigurations involves the configurational errors made by an organization against the current best practices regarding networking devices, including but not limited to network security management such as port status, unused active IP addresses, and unsecured redundancies.

Typical components scanned include virtual ports, the PostgreSQL Database, and SSL certificates. This vulnerability factor revolves around networking and network-security devices such as firewalls, routers, hubs, and switches. Furthermore, this area includes assessing routing protocols implemented in these networking devices, the update version employed, configuration enabled, and the phase-out of legacy protocols such as RIPv1 and IGRP. Although applications of advanced techniques in dynamic routing protocols such as Route Poisoning, Split Horizon, and Holddown have the capability to increase security, they can be a risk factor when improperly configured on these networking devices and their respective IP routing tables [78].

5.2.3. Software and Services

The ability of an organization to manage the software and services housed at both end and internetworking devices are assessed, including but not limited to patches, protocols, and proper configuration.

Typical components scanned include HSTS preloading, CMS, and X-XMS. Details and metadata about the patch histories of the firewall devices, endpoint hosts, and network devices have an impact on the scoring. Network scanners typically capture the operating system versions of these devices and compare them against an updated Masterfile, the National Vulnerability Database, which is maintained by the security community [79]. This factor further involves the matching/compatibility check of the hardware resources against the demand of software in a network—as any mismatch can drive a device down (e.g., device exhaustion) and in turn becomes a risk (i.e., through the Energy Resource Exhaustion Attack) performed on devices that can cause network outages and halts in organizational operations [80].

5.2.4. Web Domains

Assessment of Web domains involves tracing the vulnerabilities of an organization's primary Web domain and content management systems. It includes Web accessibility, encryptions, site certificates, and controls that promote higher security.

Typical components scanned include FTP, HTTP, IP addresses, and DNS data. The vulnerability factor revealed in this section comes from the combination of data extracted from Domain Name Servers (DNS), ICMP responses, Web servers' presence (e.g., remote login servers), and email server port 25′s reliable listening. Further included herein is the operation assessment of DNS ports TCP/UDP 53, which ensures that all externally visible DNS servers are essential and not a result of a misconfiguration. Unprotected responses may indicate the presence or absence of a device on the Internet and may pose a risk of unethical probes. These have the potential to be misused by attackers for reconnaissance and should be disabled to the most considerable extent possible [81].

5.2.5. Firmographic Information

Information about an organization's business, including financials, size, and other related categories, is considered in assessing firmographic information. Included herein are the possible surface risk for social engineering and reconnaissance-based attacks.

Typical components scanned include leaked company emails, official Web Sites, information leaks. A wide breadth of data sources may reveal attached organizational details and allow the mapping of crucial vendor management tasks—both of which are assessed in this vulnerability category since data that are set to public (typically firmographic information) can be shared in the Dark Web. Although the mere setting of these data to the public does directly cause a breach, when IP scans and reconnaissance can easily detect

this information, it can all yield insights about organizations that can be a precursor to a breach [82]. The approach of the cyber risk scoring model is sensitively conservative in the sense that while many of these indicators are not necessarily a causal factor of breach themselves, the very possibility that it may be used as a means to actual breach events can be a risk factor. Although a baseline exists, there are variations in scoring structure—which are sourced from the different industry standards, requirements, and regulations of sectors such as education, health sectors, and finance [83].

5.2.6. Historical Breaches

The corpus of past breaches involving an organization that has been reported is sought. Furthermore, it includes the assessment of the historical response undertaken against such incidents to promote business continuity.

Typical components scanned include Typosquat domains, system logs, and patch versions. In retrospect, an organization's security history is vital because threat assessors, insurers, involved partners, and attached vendors may use it to assess how an organization manages threats and performs risk mitigation. The argument is that threat may be communicative—in the sense that an organization is non-atomic and can pass on its cyber risk to its partners and be an attack surface in lieu of its affiliated organizations [84]. This vulnerability factor highlights the importance of a good record in risk response and knowledge management that pertains to cyber risks. Similar to financial credit history, this dimension is highly used to determine and predict an organization's most probable future ability to respond to risk, including novel and unprecedented ones, through a historical data-driven analysis [85,86].

6. Analysis and Results

In order to analyze the consistency and reliability of C-TPRM solutions, we conducted an analysis by gathering and comparing a set of C-TPRM reports generated by different companies for a specific organization.

6.1. The Inclusion Criteria of Cyber Rating Companies

For the inclusion criteria, the risk-scoring companies considered for inclusion in this study are all members of the Third-Party Risk Association (TPRA). Among the eligible ones, inquiries are then sent to the companies to confirm if they perform cybersecurity evaluations. Ten are formally invited to perform an analysis on the security posture of the test subject. Of the ten companies invited, only four (e.g., FICO, BitSight, RiskRecon, and ComplyScore) agreed to provide a non-intrusive scan report. The others require a placement fee prior to score assignment or prior to performing a non-intrusive scan.

6.2. Data Collection

Three of the rating companies performed a demonstration that displays the current security landscape of the subject except for FICO. This is supplemented with a hypothetical after scenario (how the score would be improved) once their solution and recommendations have been applied. Note that the rating ComplyScore assigned from the non-intrusive scan is just a part of their complete package, which involves an on-site exploration and investigation of mostly more intrusive methods, all of which will transcribe after an agreement (paid) has been reached. BitSight and RiskRecon both required live synchronous demonstration prior to the score placement of the subject. Among these, only FICO almost instantly gave the rating without any human interaction, only requiring details of the subject organization's name and Web site. Furthermore, the turn-around time is measured from the day the invitation was sent up to the report was acquired (Table 1).

Table 1. Comparison of methodologies and reports.

	FICO	BitSight	RiskRecon	ComplyScore
Upfront Scan Cost	Free	Waived	Waived	Free
Report Structure	Full	Full	Full	Partial
Demonstration Required	No	Yes	Yes	No
Turn-around Time	Instantaneous	3 days	1 week	2 weeks

6.3. Results

This section provides a summary of the comparative analysis for the results of a set of C-TPRM reports generated by different companies for a specific subject organization. Each company has a distinct approach to offer: particularly, the comprehensiveness of FICO, the exclusive benchmarked datasets of BitSight, the highly customized scoring of RiskRecon, and the management locus of ComplyScore is distinguished. As the subject for the non-intrusive assessments, the University at Albany scored differently in the evaluation of each of the C-TPRM platforms (Table 2).

Table 2. Comparison of summary of results for the University at Albany.

	FICO	BitSight	RiskRecon	ComplyScore
Max Points Possible	850	900	10	100
Score Garnered	482	540–570 (Range)	6.8	80
Interpretation	High Risk	Basic-Bottom 30% of Education	Bottom 20% of Education	B (Letter Grade)
Normalized Score	57%	60–63%	68%	80%
Solution Pricing	Subscription	Subscription	Subscription	Subscription

6.3.1. FICO's Report

FICO reported the lowest score for the subject as their model tests the organization against use cases that involves a collection of highly diverse cross-sectional measurements. As per metric scale interpretation, the subject belongs to the group with the highest risk of experiencing a data breach. The score stemmed from considering the poor performance of service and configuration risk of the poorest network prefix. This includes a high number of devices or services that have been observed responding to TCP, UDP, or ICMP probes. Moreover, the subject displayed evidence that the content of Web resources may be out of date or misaligned with current privacy standards and regulations.

6.3.2. BitSight's Report

With a small degree of deviation, BitSight reported a slightly higher risk score. The subject again consistently scored low on endpoint behaviors, i.e., access device tests. BitSight reported that spam propagation and botnet infections are highly likely to occur and that some devices are potentially exploited. Likewise, Web resources consistently contributed to the low performance, mainly due to poor Web headers, unsecured open ports, and out-of-date SSL certificates. Interestingly, the SSL configuration score was interpreted relatively high within the specific industry to which the subject belongs, in this context—education.

6.3.3. RiskRecon's Report

The report issued by RiskRecon also resulted in poor performance of Web applications of the subject. The subject specifically scored 2.2 out of 10 for Web applications, and as per suggestion, it requires immediate halt and re-assessment on this domain. Issues for this component are primarily attributed to HTTPS security headers and content management authentication problems. Surprisingly, and as a counterargument for BitSight, the subject scored high (8.6/10) for the Web encryptions component, with an industry average of 8.2. From the 810 pre-defined tests, only 40 issues were found. These tests include certificates

and encryption protocols. On the other side of the spectrum, the subject scored perfectly (10 out of 10) on data loss events (i.e., historical breach) and threat intelligence (i.e., the possible state of current compromises inside the organizational system).

6.3.4. ComplyScore's Report

Finally, ComplyScore reported the highest score on the subject. However, this evaluation is only an initial score generated, as ComplyScore performs a rigorous assessment before a final score can be awarded on the organization since their primal locus is management and compliance of an organization against current standards, laws, and benchmarked security policies. As per the supporting documents, their risk assessment is built around a questionnaire supplemented by telephonic conversations or email correspondence as necessary. The subject scored poorly due to possibly unpatched Web Servers and Operating Systems. The Trustworthiness score is 100/100—with the implication of no infections in the past 12 months, although a spam zero-day is detected five years back. However, an important disclaimer on the report is that the validation of any special contractual requirements is not part of the scope of this assessment.

Based on three out of four different C-TPRM reports, it is seen that the subject organization is determined as high risk and ranked at the bottom of the education sector. Only the results of ComplyScore provide a high score for the subject organization, and it is explained as due to their primal locus being management and compliance.

7. Discussion

C-TPRM is a relatively new but developing and high-demand concept in the business world, especially in line with its utilization in the cyber insurance sector. Today, every vendor or partner organization possesses a potential security risk. Even if an organization has the best cybersecurity in the world, its data, customers, and reputation are at risk of suffering a cyber incident caused by a third party.

In this research, we gathered the existing methods for C-TPRM developed by different companies, presented the commonly used indicators and criteria for the assessments, and compared the results of different methods for a specific organization. Seminal findings include the revelation that variations exist in the assessment by the different cyber risk scoring companies. Moreover, this study attempted to trace where these inconsistencies are sourced. This article's findings suggest that these are significantly sourced from the differences in evaluation methodologies, the inclusion of proprietary datasets, and consideration of additional risk factors beyond the common baseline and metrics. There is a need for standardization from data collection to risk score calculation to have reliable and consistent results similar to credit scores.

The significance of this article is through its contribution to the research stream of Cyber Risk Predictive Modeling. Findings indicate that more analyses that include C-TPRM reports for a larger sample of multiple subject organizations should be performed to evaluate the consistency of the scoring companies through statistical tests further to reach a common ground. Certainly, a high degree of uniformity in ratings among the different risk scoring companies would suggest the stability of C-TPRM as a whole. The practical significance of this study is the awareness it brings to the key people involved in acquiring security scoring for their organizations—that not a single security rating will dictate the current state and picture of the security posture of an organization. Furthermore, this article suggests that companies should consider having their security landscape be assessed by more than one rating company for a more thorough picture of their security posture relative to the industry to which they belong.

8. Conclusions

The emergence of C-TPRM has certainly filled in the gap where it is needed the most—the need for an empirical, data-driven assessment of an organization's current security landscape. This is significantly due to the need to estimate an organization's

unit risk—the risk an organization carries by itself. When an organization, typically functioning as a vendor, is connected to other organizations, it can proliferate that unit risk to its attached organizations. However, the current state of C-TPRM dictates that more improvement can be made to maximize its potential—particularly in the area of risk scoring, the methodologies it is anchored on, and the convergence of the datasets used.

Further research is required to assess, more accurately, the reliability and consistency of C-TRPM scores produced by different companies. This analysis is essential to show if a score is a reliable indicator of risk posed by a vendor. To conduct a reliability and consistency analysis, first, we need a larger dataset of risk scores for different companies. As shown in Table 2, the data are in a qualitative form (a report) and have different representations. In order to compare and analyze data in various formats, this data should be coded in a quantitative form and normalized. Normalization eliminates the units of measurement for data and enables us to compare data from different sources using the same scale. Later, normalized data should be analyzed using statistical techniques. To analyze the consistency of overall risk scores, ANOVA can be used. To compare overall scores by considering the factors used for overall risk score calculation, MANOVA will be helpful. For each of these analyses, post hoc tests should follow. This comparison analysis can also help create a risk score equation, which will be based on weighted risk scores obtained from selected risk scoring companies.

Author Contributions: Conceptualization, U.T., O.F.K., and I.T.; methodology, U.T. and I.T.; validation, O.F.K., K.M.C., and I.T.; formal analysis, K.M.C. and O.F.K.; investigation, K.M.C., O.R., I.T., and O.F.K.; resources, K.M.C. and O.R.; data curation, K.M.C., O.F.K. and I.T.; writing—original draft preparation, O.F.K., K.M.C., I.T., O.R., and U.T.; writing—review and editing, U.T. and O.F.K.; visualization, K.M.C. and O.F.K.; supervision, U.T.; project administration, U.T.; funding acquisition, U.T. All authors have read and agreed to the published version of the manuscript.

Funding: This material is partially based upon work supported by the National Science Foundation under Grant No. (1948261).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Collier, Z.A.; Hassler, M.L.; Lambert, J.H.; DiMase, D.; Linkov, I. Supply Chains. In *Cyber Resilience of Systems and Networks*; Kott, A., Linkov, I., Eds.; International Publishing Springer: Cham, Switzerland, 2019; pp. 447–462.
2. Kalogeraki, E.M.; Papastergiou, S.; Mouratidis, H.; Polemi, N. A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments. *Appl. Sci.* **2018**, *8*, 1477. [CrossRef]
3. Brandis, K.; Dzombeta, S.; Colomo-Palacios, R.; Stantchev, V. Governance, Risk, and Compliance in Cloud Scenarios. *Appl. Sci.* **2019**, *9*, 320. [CrossRef]
4. The ROI of Supply Chain Resiliency: It's More Than You Think. Resilinc. November 2013. Available online: https://info.resilinc.com/roi-of-supply-chain-resiliency-resilinc-sourcing-innovation (accessed on 20 June 2019).
5. Managing Cyber Risks in an Interconnected World KEY Findings from The Global State of Information Security Survey 2015. PwC. September 2014. Available online: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (accessed on 20 June 2019).
6. Data Risk in the Third-Party Ecosystem. Ponemon Institute. September 2017. Available online: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/sep2017/cs2017_0340.pdf (accessed on 18 February 2021).
7. Korolov, M. What Is a Supply Chain Attack? Why You Should Be Wary of Third-Party Providers, CSO Online. 25 January 2019. Available online: https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html (accessed on 19 June 2019).
8. Kaplan, S.; Garrick, B.J. On The Quantitative Definition of Risk. *Risk Anal.* **1981**, *1*, 11–27. [CrossRef]
9. Sailio, M.; Latvala, O.M.; Szanto, A. Cyber Threat Actors for the Factory of the Future. *Appl. Sci.* **2020**, *10*, 4334. [CrossRef]
10. Karabacak, B.; Tatar, Ü. Strategies to Counter Cyber Attacks: Cyber Threats and Critical Infrastructure Protection. In *Critical Infrastructure Protection*; IOS Press: Amsterdam, The Nederlands, 2014; Volume 116, p. 19.
11. National Institute of Standards and Technology. Minimum Security Requirements for Federal Information and Information Systems, FIPS PUB 200. March 2006. Available online: https://csrc.nist.gov/publications/detail/fips/200/final (accessed on 11 December 2020).
12. Gritzalis, D.; Stergiopoulos, G.; Vasilellis, E.; Anagnostopoulou, A. Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud. In *Advances in Core Computer Science-Based Technologies*; Springer: Cham, Switzerland, 2021.

13. Syalim, A.; Hori, Y.; Sakurai, K. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. In Proceedings of the 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan, 16–19 March 2009; pp. 726–731. [CrossRef]
14. Gritzalis, D.; Iseppi, G.; Mylonas, A.; Stavrou, V. Exiting the Risk Assessment Maze. *ACM Comput. Surv.* **2018**, *51*, 1–30. [CrossRef]
15. Tatar, Ü.; Karabacak, B. An hierarchical asset valuation method for information security risk analysis. In Proceedings of the International Conference on Information Society (i-Society 2012), London, UK, 25–28 June 2012; pp. 286–291.
16. Bahsi, H.; Udokwu, C.; Tatar, U.; Norta, A. Impact Assessment of Cyber Actions on Missions or Business Processes-A Systematic Literature Review. In Proceedings of the ICCWS 2018 13th International Conference on Cyber Warfare and Security, Washington, DC, USA, 8 March 2018.
17. National Institute of Standards and Technology. Managing Information Security Risk Organization, Mission, and Information System View; NIST SP 800-39. March 2011. Available online: https://csrc.nist.gov/publications/detail/sp/800-39/final (accessed on 14 February 2021).
18. National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy. NIST SP 800-37 Revision 2. December 2018. Available online: https://doi.org/10.6028/NIST.SP.800-37r2 (accessed on 14 February 2021).
19. National Institute of Standards and Technology. Guide for Conducting Risk Assessment, NIST SP 800-30 Revision 1. September 2012. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 14 February 2021).
20. International Standards Organization. Information Security Management, ISO/IEC 27001. October 2013. Available online: https://www.iso.org/isoiec-27001-information-security.html (accessed on 11 December 2020).
21. International Standards Organization. Information Technology—Security Techniques—Information Security Risk Management, ISO/IEC 27005:2018. July 2018. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html (accessed on 11 December 2020).
22. Tatar, U.; Gheorghe, A.V.; Gokce, Y. (Eds.) *Strategic Cyber Defense: A Multidisciplinary Perspective*; IOS Press: Amsterdam, The Netherlands, 2017.
23. Handfield, R.B.; Bechtel, C. The role of trust and relationship structure in improving supply chain responsiveness. *Ind. Mark. Manag.* **2002**, *31*, 367–382. [CrossRef]
24. Mora-Monge, C.; Quesada, G.; Gonzalez, M.E.; Davis, J.M. Trust, power and supply chain integration in Web-enabled supply chains. *Supply Chain Manag. Int. J.* **2019**, *24*, 524–539. [CrossRef]
25. Li, S.; Wang, N.; Du, X.; Liu, A. Internet Web Trust System Based on Smart Contract. In *Data Science*; Springer: Singapore, 2019; pp. 295–311. [CrossRef]
26. Sillence, E.; Blythe, J.M.; Briggs, P.; Moss, M. A Revised Model of Trust in Internet-Based Health Information and Advice: Cross-Sectional Questionnaire Study. *J. Med. Internet Res.* **2019**, *21*, e11125. [CrossRef] [PubMed]
27. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 746–789. [CrossRef]
28. Ghadge, A.; Weiß, M.; Caldwell, N.D.; Wilding, R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Manag. Int. J.* **2019**, *25*, 223–240. [CrossRef]
29. Drakopoulos, G.; Kafeza, E.; Al Katheeri, H. Proof Systems In Blockchains: A Survey. In Proceedings of the 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, 20–22 September 2019; pp. 1–6. [CrossRef]
30. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
31. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to Scalability of Blockchain: A Survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
32. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
33. Alla, S.; Soltanisehat, L.; Tatar, U.; Keskin, O. Blockchain Technology in Electronic Healthcare System. In Proceedings of the 2018 IISE Annual Conference, Orlando, FL, USA, 19–22 May 2018.
34. Pour, F.S.A.; Tatar, U.; Gheorghe, A. Agent-Based Model of Sand Supply Governance Employing Blockchain Technology. In Proceedings of the 2018 Spring Simulation Multi-Conference, Baltimore, MD, USA, 15–18 April 2018. [CrossRef]
35. Tatar, U.; Gokce, Y.; Nussbaum, B. Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Comput. Law Secur. Rev.* **2020**, *38*, 105454. [CrossRef]
36. Boyson, S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation* **2014**, *34*, 342–353. [CrossRef]
37. Warren, M.; Hutchinson, W. Cyber attacks against supply chain management systems: A short note. *Int. J. Phys. Distrib. Logist. Manag.* **2000**, *30*, 710–716. [CrossRef]
38. Boyson, S.; Corsi, T.; Rossman, H. *Building a Cyber Supply Chain Assurance Reference Model*; Science Applications International Corporation (SAIC): Reston, VA, USA, 2009.
39. Storch, T. *Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity*; Microsoft Corporation: Albuquerque, NM, USA, 2011; pp. 7–9.

40. Heinbockel, W.J.; Laderman, E.R.; Serrao, G.J. *Supply Chain Attacks and Resiliency Mitigations*; The MITRE Corporation: Dranesville, VA, USA, 2017; p. 82.
41. Boyens, J.M.; Paulsen, C.; Moorthy, R.; Bartol, N. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*; NIST SP 800-161; National Institute of Standards and Technology: Gaithersburg, MD, USA, April 2015. [CrossRef]
42. McDaniel, E.; Albert, M.; Cohen, B.; Ortiz, C.J. *Making Smart Decisions About Supply Chain Security in the Age of Globalization*; Sponsored Report Series; Acquisition Research Program: Monterey, CA, USA, 2017; p. 21.
43. Shu, X.; Tian, K.; Ciambrone, A.; Yao, D. Breaking the Target: An Analysis of Target Data Breach and Lessons Learned, arXiv:1701.04940 [cs]. January 2017. Available online: http://arxiv.org/abs/1701.04940 (accessed on 18 June 2019).
44. McCoy, K. Target to pay $18.5M for 2013 data breach that affected 41 million consumers. *USA Today*. 23 May 2017. Available online: https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ (accessed on 1 November 2020).
45. A 'Kill Chain' Analysis of the 2013 Target Data Breach, U.S. Senate. March 2014. Available online: https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883 (accessed on 10 September 2020).
46. Radichel, T. Case Study: Critical Controls that Could Have Prevented Target Breach, SANS Institute. September 2014. Available online: https://www.sans.org/reading-room/whitepapers/casestudies/paper/35412 (accessed on 15 March 2021).
47. Banjo, S. Home Depot Hackers Exposed 53 Million Email Addresses. *Wall Str. J.* 2014. Available online: https://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282(accessed on 11 October 2020).
48. Seals, T. Home Depot to Pay $27.25m in Latest Data Breach Settlement. *Infosecurity Magazine*. 13 March 2017. Available online: https://www.infosecurity-magazine.com:443/news/home-depot-to-pay-2725m/ (accessed on 1 November 2020).
49. Hawkins, B. Case Study: The Home Depot Data Breach, SANS Institute. January 2015. Available online: https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367 (accessed on 11 October 2020).
50. U.S. Office of Personnel Management. About Us, U.S. Office of Personnel Management, Washington, DC, USA. Available online: https://www.opm.gov/about-us/ (accessed on 5 March 2021).
51. Kennel, D. *OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster*; SANS Institute: North Bethesda, MD, USA, 29 March 2016.
52. Chabrow, E. DHS Responds to RSA SecurID Breach. *Bankinfo Security*, 18 March 2011.
53. Hoffman, S. RSA SecureID Breach Costs EMC $66 Million, CRN. 28 July 2011. Available online: https://www.crn.com/news/security/231002862/rsa-secureid-breach-costs-emc-66-million.htm (accessed on 15 February 2021).
54. Richmond, R. The RSA Hack: How They Did It. *Bits Blog*. 2 April 2011. Available online: https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/ (accessed on 1 February 2021).
55. Williams, J. What You Need to Know About the SolarWinds Supply-Chain Attack, SANS Institute. 15 December 2020. Available online: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ (accessed on 17 February 2021).
56. FireEye. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUN-BURST Backdoor. *FireEye Threat Research*. 13 December 2020. Available online: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html (accessed on 17 February 2021).
57. Barrett, B. Russia's SolarWinds Hack Is a Historic Mess. *Wired*, 19 December 2020.
58. Paul, K. What you need to know about the biggest hack of the US government in years. *The Guardian*, 15 December 2020.
59. Whitaker, B. SolarWinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments. *CBS News*. 14 February 2020. Available online: https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/ (accessed on 17 February 2021).
60. Newman, L.H. The SolarWinds Hackers Used Tactics Other Groups Will Copy. *Wired*, 19 January 2021.
61. Weiss, J.; Hunter, B. The SolarWinds Hack Can Directly Affect Control Systems. *Lawfare*. 22 January 2021. Available online: https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems (accessed on 17 February 2021).
62. Miller, M.; Chalfant, M. Biden to take 'executive action' to address SolarWinds breach. *The Hill*, 17 February 2021.
63. Brewster, T. SolarWinds Hacks: Virginia Regulator And $5 Billion Cybersecurity Firm Confirmed as Targets. *Forbes*. 25 January 2021. Available online: https://www.forbes.com/sites/thomasbrewster/2021/01/25/solarwinds-hacks-virginia-regulator-and-5-billion-cybersecurity-firm-confirmed-as-targets/ (accessed on 17 February 2021).
64. Newman, L.H. A Second SolarWinds Hack Deepens Third-Party Software Fears. *Wired*, 2 February 2021.
65. BitSight Technologies Inc. BitSight vs. Competitors-Security Ratings Alternatives, BitSight. Available online: https://www.bitsight.com/bitsight-vs-competitors (accessed on 12 December 2020).
66. BitSight Technologies Inc. Understand Your Security Rating | BitSight Security Ratings, BitSight. Available online: https://www.bitsight.com/understand-your-rating (accessed on 12 December 2020).
67. Atlas Systems ComplyScore signs partnership with Qualys, Atlas Systems: Database, Big Data, Cloud, Oracle, SAP. Available online: https://www.atlassystems.com/recent-update_news/complyscore-signs-partnership-with-qualys/ (accessed on 11 December 2020).
68. Carrns, A. Is That Credit Score a FICO, or a FICO 8? *Bucks Blog*. 10 May 2012. Available online: https://bucks.blogs.nytimes.com/2012/05/10/is-that-credit-score-a-fico-or-a-fico-8/ (accessed on 12 December 2020).

69. FICO Named Cyber Risk Quantification Category Leader for Second Year Running. Available online: https://www.prnewswire.com/news-releases/fico-named-cyber-risk-quantification-category-leader-for-second-year-running-301132954.html (accessed on 17 December 2020).
70. Allgeier, H. Jennifer Bisceglie Honored as EY Entrepreneur of The Year®2020 Mid-Atlantic Award Finalist, Interos Inc. 27 August 2020. Available online: https://www.interos.ai/bisceglie-ey-entrepreneur-of-the-year/ (accessed on 12 December 2020).
71. Recorded Future. The Threat Intelligence Company. 2020. Available online: https://www.recordedfuture.com/about/ (accessed on 12 December 2020).
72. Miller, R. Mastercard Acquires Security Assessment Startup, RiskRecon, TechCrunch. Available online: https://social.techcrunch.com/2019/12/23/mastercard-acquires-security-assessment-startup-riskrecon/ (accessed on 12 December 2020).
73. NormShield. Cyber Risk Rating System. 4 August 2020. Available online: https://normshield.com/platform/ (accessed on 12 December 2020).
74. Klugerman, Y. Panorays' Revolutionary 3rd Party Security Ratings Model and Additional Key Features. *Panorays*. 22 July 2020. Available online: https://www.panorays.com/blog/panorays-introduces-revolutionary-third-party-security-ratings-model-and-additional-key-features/ (accessed on 12 December 2020).
75. SecurityScorecard. Third-Party Risk Management (TRPM) Solutions. 2020. Available online: https://securityscorecard.com/solutions/use-cases/third-party-risk-management (accessed on 12 December 2020).
76. Fasulo, P. SecurityScorecard 10 Risk Factors Explained, SecurityScorecard. 2 November 2020. Available online: https://securityscorecard.com/blog/securityscorecard-10-risk-factors-explained (accessed on 13 December 2020).
77. Papadaki, M.; Furnell, S. IDS or IPS: What is best? *Netw. Secur.* **2004**, *2004*, 15–19. [CrossRef]
78. Verma, A.; Bhardwaj, N. A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol. *Int. J. Futur. Gener. Commun. Netw.* **2016**, *9*, 161–170. [CrossRef]
79. Li, F.; Paxson, V. A Large-Scale Empirical Study of Security Patches. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 2201–2215.
80. Desnitsky, V.; Kotenko, I. Modeling and Analysis of IoT Energy Resource Exhaustion Attacks. In *Econometrics for Financial Applications*; Springer Science and Business Media LLC: Berlin, Germany, 2017; Volume 737, pp. 263–270.
81. Garfinkel, S.; Spafford, G. *Web Security, Privacy and Commerce*, 2nd ed. Expanded & Updated; O'Reilly Meida, Inc.: Cambridge MA, USA, 2002.
82. Evans, A. *Managing Cyber Risk*; Routledge: London, UK, 2019.
83. Sohval, B. *A Deep Dive in Scoring Methodology*; SecurityScorecard Inc.: New York, NY, USA, 2020.
84. Olcott, J. *Input to the Commission on Enhancing National Cybersecurity: The Impact of Security Ratings on National Cybersecurity*; BitSight Technologies: Boston, MA, USA, September 2016.
85. Liu, Y.; Sarabi, A.; Zhang, J.; Naghizadeh, P. Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In Proceedings of the 24th {USENIX} Security Symposium ({USENIX} Security 15), Washington, DC, USA, 12–14 August 2015; pp. 009–1024.
86. Sarabi, A.; NaghiZadeh, P.; Liu, Y.; Liu, M. Risky business: Fine-grained data breach prediction using business profiles. *J. Cybersecur.* **2016**, *2*, 15–28. [CrossRef]