THIRD PARTY RISK MANAGEMENT (TPRM):

IN A PERFECT WORLD

AUTHOR:

CHARLES KOLODGY

TABLE OF CONTENTS

© SECURITY CURRENT 2020

IN A PERFECT WORLD

In a perfect world, Chief Information Security Officers (CISO) would utilize every resource at their fingertips to secure enterprises against any potential threat and vulnerability. It's no secret we don't live in a perfect world. Consider the proliferation of systems, immense amounts of sensitive data, too many exploits and adversaries, and a shortage of trained security professionals. The CISO sits in the unenviable position of determining protection for these critical systems and what information is required to run a modern enterprise. Further, they need to be armed to defend these decisions.

In efforts of delivering findings, it's imperative a CISO presents each plan in terms company executives understand and appreciate. As a CISO and team work to align the common goal of growing the company's bottom line, the cyber risk must be quantified in order to optimize threat protection in every security investment decision. Enterprises rely on sophisticated computing equipment to remain competitive. This technology has potential to bring forth innovation and productivity improvements that benefit the business. Maintaining security of these systems is required, but comes at a cost. While proving the value of this cost, the CISO must move beyond a general view of risk management to one that is granular and speaks for itself in prioritizing above alternate activities.

This paper will discuss how cyber risk management is perceived and explain a new method of calculating risk paralleling with other forms of business risk management. It will concentrate on inherent risks in a network and application infrastructure with a myriad of connections to outside partners, suppliers, and service providers. A CISO does not have direct control over the security provided by third parties, highlighting the responsibility of assessing the risk of corporate information accessible from each third party's network. The risk management process needs to be consistent and identify a quantifiable risk to the organization. The paper concludes with a compelling discussion on how NormShield can help CISOs quantify risks that emerge from third parties.

MAKING THE TOUGH DECISIONS

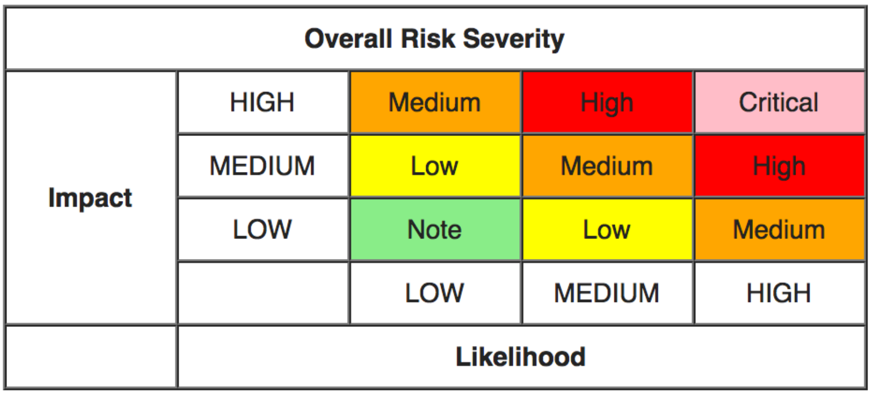
Most business processes rely on some level of IT infrastructure to operate. These structures are skyrocketing in complexity due to advances in cloud, mobile, and networking technology. All of these factors multiply the attack surface, making security more difficult. Adversaries have a knack for finding the weakest link, and with a more exposed attack surface the cybersecurity vulnerability to the business increases significantly. There is no debate that an enterprise's information technology infrastructure (systems, storage operations, network connectivity, endpoints, and applications) must be protected from adversaries who want to steal from or impose some other harm upon the entity.

Organizations spend between 6-12% of their IT budget on cyber security products and services. Unfortunately, this spending is not an accurate measure of success nor does it fully protect an organization from data breaches. According to the Ponemon Institute's Cyber Risk Index, 73% of businesses experienced some type of infiltration into their network while over 60% of businesses suffered a breach of customer data or lost sensitive intellectual property over the previous 12 months. One of the reasons this spending doesn't keep the enterprise completely safe falls on the nonexclusive selection of security products. Certain types of security components, such as firewalls, endpoint security, access control, anti-virus, and vulnerability management are expected. While they are certainly required, the way they are deployed may not be optimized for the enterprise's specific environment. Some security technologies are purchased as the "shiny new toy" which came about in response to the latest security headline. CISOs realize they must make the tough decisions regarding the prioritization in protecting their critical data, while taking into account the business and operational impact, not just the security needs.

Compliance, uncertainty, and fear often fuel security decisions, but realizing the potential business advantages of information security requires a consistent, repeatable, and manageable threat-mitigation and risk management process. CISOs can use a tenacious risk management process to run a proactive and optimum cyber security program. This program can identify the real value of security and assess and make adjustments when technology and events change the risk posture, while avoiding snap judgements. The challenge is understanding what cyber risk is and how best to measure its impact in business terms.

DEFINING CYBER RISK

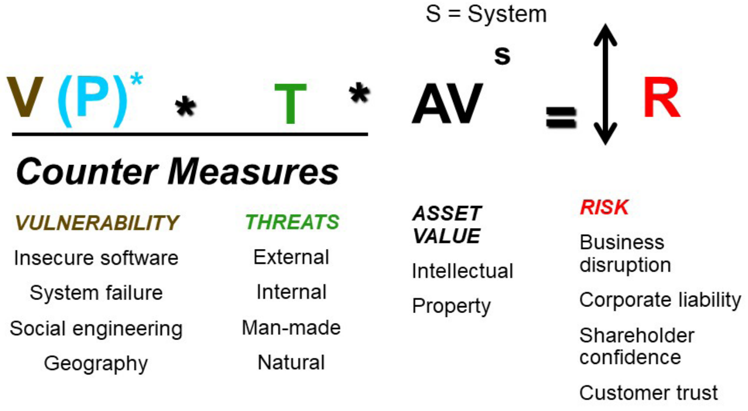
We take a risk in everything we do. Every time we get into a car, cross the street, and even the relationships we build with others every day. But what does risk really mean? People sometimes misuse the word "risk", when "threat" would be more contextual. Generally speaking, people use the term "risk" when they want to convey something scary, while using it interchangeably with threats, control deficiencies, and loss. There are many different categories of risks, but what is most relative to this discussion are Business Risk and Information Security Risk. A simple definition of business risk is the exposure a company has to external or internal factors that will have a significant impact on profits or can lead to a specific or general failure. Another way of looking at it is anything that threatens a company's ability to meet its financial goals is a business risk. Companies have learned to limit their risk exposure by adopting a risk management strategy that identifies the risks, how those risks could impact the organization and what controls are in place to mitigate those risks. The organization's risk management process is part of the Integrated Risk Management (IRM) which coordinates a strategy for corporate governance, enterprise risk management, and corporate compliance with government regulations. Generally organizations understand the value IRM brings to the organization. From there, they can measure the financial impact of potential events and evaluate if they can tolerate a particular risk based on their level of risk acceptance.



Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

The definition of Information Security Risk takes a much more simplistic view. NIST FIPS 200 and ISO 27001 provide a similar explanation, claiming it's a combination of a threat actor's ability to exploit a vulnerability within an information asset and the potential impact this event could have on the organization. As illustrated in Figure 1, cyber risk is often expressed using levels of Critical, High, Medium, or Low and portrayed using red, yellow, and green colored tags.

Fundamental Risk Equation



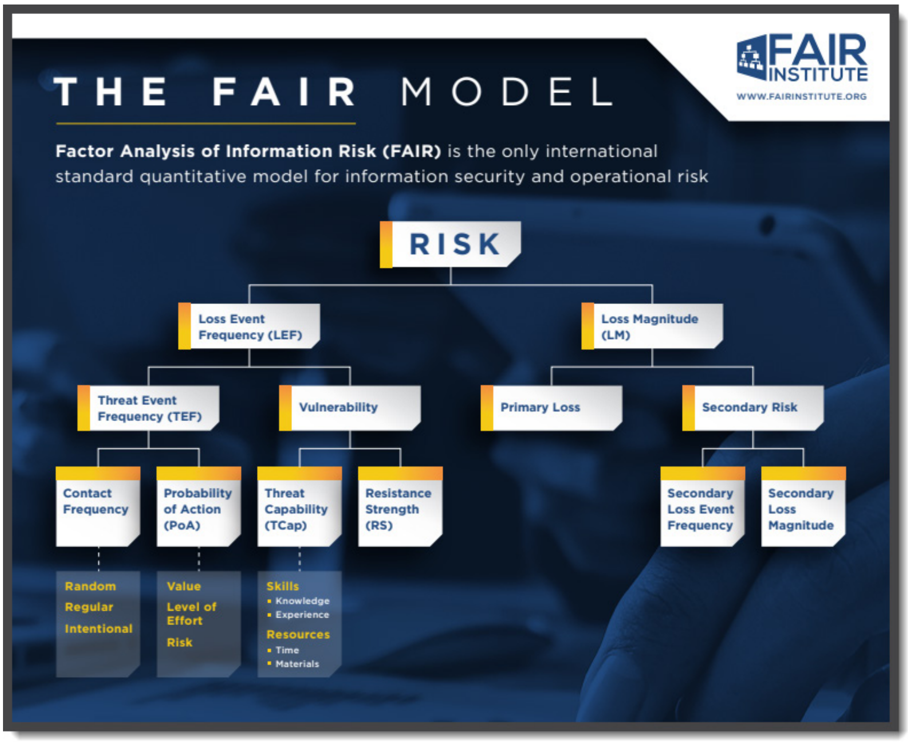
* PROBABILITY = Popularity X Exposure

The imprecise nature of cyber security risk measurement, based on risk matrices, is not conducive to making logical and comprehensive cyber risk mitigation decisions. Instead, unmeasured risk perpetuates the concept of FUD: Fear, Uncertainty, and Doubt. FUD has been the hallmark of many security discussions. To make it worse, people have a tendency of overestimating risks and confusing perceived threats with real threats, making real measurement even more difficult. This lack of precision does not provide clarity when the CISO discusses overall cyber risk and the need for security resources with company executives. Corporate boards, executives, and risk managers are demanding more information on how cyber risk impacts the company in business and economic terms. Security professionals have tried to create models to solve the checklist view of cyber risk management. One such equation is presented in Figure 2. It attempts to provide additional granularity by emphasizing the probability that a vulnerability will be exploited, the impact countermeasures have in mitigating risk, and how the asset value contributes to the overall risk calculation. Although a step in the right direction, it is only an example of what could be done to allow cyber risk management to conform to the larger corporate risk program.

A more comprehensive method measuring cyber security risk in business terms is called Factor Analysis of Information Risk (FAIR™). FAIR™ is an internationally recognized standard risk taxonomy and risk quantification model. CISOs who incorporate this model into their threat-mitigation and risk-management process gain the ability to calculate the probable financial impact if a cyber event were to occur. Being able to manage cyber security risk in both business and economic terms allows for a better prioritization of risk and more effective allocation of resources. It is possible to quantifiably evaluate which risk mitigation strategies are most effective in reducing risk, and the options can be presented based on a cost benefit analysis instead of with a color coded matrix. Ultimately FAIR™ allows the CISO to speak the same language as others involved in the enterprise's risk efforts.

FACTOR ANALYSIS OF INFORMATION RISK (FAIR™)

FAIR provides a structured, valid and recurring model for cyber risk quantification. It counteracts security FUD (Fear, Uncertainty, and Doubt) by providing a measurement model for understanding, analyzing, and quantifying information risk in financial terms. By adopting FAIR, organizations have a foundation upon which to build a robust information risk management approach. FAIR helps to fill the gaps in other risk management frameworks by providing a proven and standard risk quantification methodology that can be leveraged within other risk management programs. There are a number of standards that prescribe the need to quantify risk, but they do not provide specifics on how risk should be calculated. In contrast, the FAIR model is specifically designed to support risk quantification. Communities have begun to realize FAIR's process can improve risk analysis ensuring FAIR can complement other standards. Along those lines, the National Institute of Standards and Technology (NIST) published an Informative Reference to the NIST Cybersecurity Framework, the most widely used cybersecurity framework in the U.S. The Informative Reference provides a mapping between FAIR and the NIST CSF standard in the sections covering risk analysis and risk management.



FAIR provides the following components:

- A standard taxonomy for information and operational risk
- Data collection criteria
- Measurement scales for risk factors
- A modeling construct for analyzing complex risk scenarios

In calculating risk, the FAIR model's key components are Loss Event Frequency (LEF) and Loss Magnitude (LM). Loss Magnitude (LM) essentially answers the question, "What will be the impact if there is a breach," while Loss Event Frequency (LEF) calculates the likelihood of a breach. Figure 3 provides a visual representation of the additional elements used to calculate the LEF and LM. Additional detail on FAIR is available from the FAIR Institutes website (https://www.fairinstitute.org/what-is-fair)

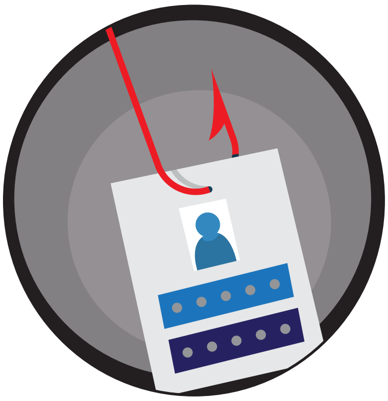
WITH FRIENDS LIKE THAT ...

As CISOs build out their risk management program, it's imperative they do not forget to incorporate risks posed by third party partners. Gone are the days when an organization held all of their critical information in-house. Today, everything is distributed using remote access and cloud-based technologies, requiring firms to rely on a complex web of partners and services to operate. According to a survey conducted by Bomgar, an average of 181 external vendors and suppliers are granted access to a company's business systems each week. Some of the largest organizations might deal with more than one thousand different entities in a year. The number of third parties granted access to network resources continues to grow.

Organizations have their assets, including business information, spread amongst many locations in the cloud. It's difficult to know exactly where data resides by location or what end party is holding or has access to that material. All of this sharing expands the attack surface and widens the organization's risk exposure.

When author Joey Adams said, "With friends like that, who needs enemies," he didn't have the internet in mind. The organizations directly linked to your network holding private information can be the source of a damaging security breach. The third-party ecosystem is the perfect hunting ground for cyber criminals who are searching for avenues to infiltrate an organization. The larger and more complex the network, the greater the risk. The statistics already conclude this ecosystem is a problem. According to the Ponemon Institute's third annual "Data Risk in the Third-Party Ecosystem" study, 61% of respondents from American companies say they experienced a third-party breach. Three other surveys (conducted by Soha System, Bomgar, and Spiceworks) provided similar data. The first two also reported over 60% of all data breaches could be linked directly or indirectly to access provided by contractors and suppliers, while the latter survey claimed 44% of the responding firms experienced a significant, business altering data breach caused by a vendor.

BELOW ARE SOME EXAMPLES OF HOW AN ORGANIZATION'S INFORMATION CAN BE COMPROMISED BY A THIRD-PARTY VENDOR:



iPR Software, a marketing and digital publishing company, exposed the data of hundreds of their high profile clients. This includes Fortune 500 firms, well known consumer brands, and state government entities. The terabyte of information was discovered by a security researcher who found the files in an unprotected cloud data repository. It included 477,000 media contacts, business entity account information, thousands of user password hashes, other assorted documents including emails, and even system administrator credentials. It took iPR Software over a month to secure the information after they were informed of the discovery.

Medical testing organizations, LabCorp and Quest Diagnostics, had personal and financial data on millions of customers exposed when third-party billing collection firm American Medical Collection Agency's (AMCA) payment website was compromised by hackers. AMCA is a debt collection agency for many entities including hospitals, direct marketers, telecom companies, and state and local toll authorities. Information exposed by the hack of AMCA included credit card numbers, bank account information, and social security numbers. It was reported that the AMCA website had been available to hackers from August 2018 until March 2019. Both LabCorp and Quest Diagnostics reported that AMCA was not forthcoming in providing detailed information regarding the breach.

An Elasticsearch server containing a cache of loan and mortgage agreements, repayment schedules, and other sensitive financial and tax documents from leading financial institutions was left unprotected. It wasn't immediately known who owned the data, but following an investigation, it was discovered that data and analytics company Ascension, had ownership. One of the services Ascension offers is to convert paper documents and handwritten notes into computer-readable files. It was a repository of converted documents that was exposed. This incident was attributed to a server configuration error.

Nuance Communications reported in an SEC filing that certain reports hosted on a single Nuance transcription platform were accessed by an unauthorized employee. Up to 45,000 patient records which contained names, birth dates, medical record numbers, patient numbers, and dictated notes were potentially exposed. The notes included providers' assessments of patients, diagnoses, dates of service, and treatment and care plans. The stolen data was recovered by law enforcement and there was no evidence that the private healthcare information was disseminated. Nuance notified all customers who used the platform to allow them to issue notifications to affected individuals.

Supermarket chain Wegmans sued one of their suppliers who fell victim to a cyberattack that may have cost the grocer hundreds of thousands of dollars. In the filing, Wegmans accused seafood supplier Invermar of poor cybersecurity practices that allowed hackers to compromise Invermar's email system. Ultimately the cybercriminals re-directed payments Wegmans made to Invermar into their own bank accounts. Although it is unknown exactly what Wegmans actual losses were, they requested a least $900,000 in damages from Invermar. Wegmans eventually dropped the suit.

Lowe's, the building supply company, reported that information, including names, addresses, birthdays, Social Security numbers, driver's license numbers, and driving records, on current and former drivers was compromised after a third-party vendor exposed it to the public. The data was housed in E-DriverFile, an online database provided by SafetyFirst, a driver safety firm. It was reported that the root cause of the breach was in improperly secured backup.

These incidents are just a handful of examples that prove that data in the hands of third-party vendors is susceptible to leaks. The complexity of data sharing among businesses leaves a lot of gaps in security. It is imperative that CISOs have a handle on knowing how well their partners protect sensitive data.

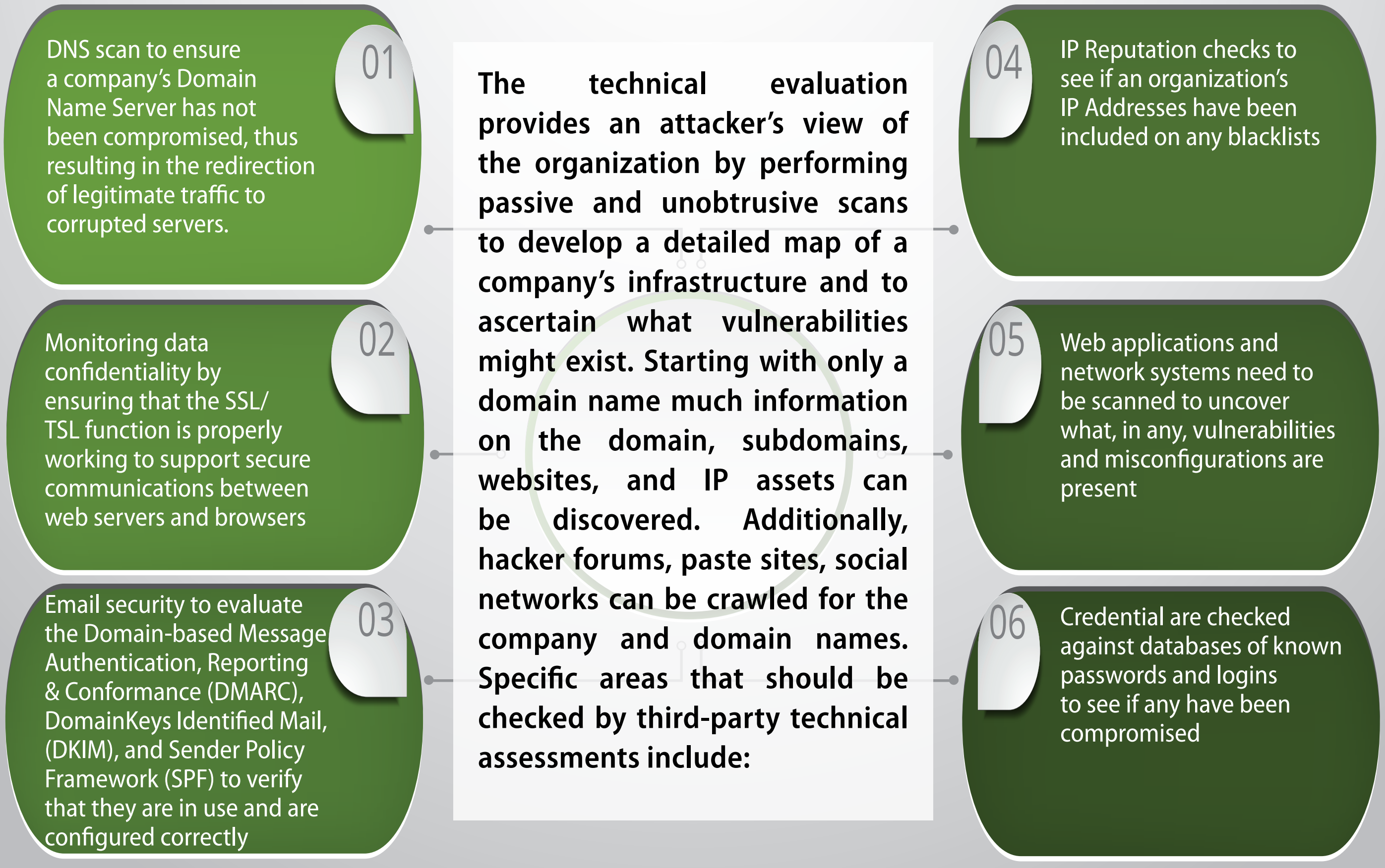
IT TAKES **WORK**

Cyber criminals are very good at their trade. They are ingenious, inventive, and unrelenting but they are also lazy as they are always searching for the path of least resistance. They have great visibility on what types of connections and assets are directly available through the open internet. As mentioned, one of the alternative means for infiltrating systems and stealing valuable data is to enter an ultimate target's third party partner. This method, provides the adversary an opportunity to enter the network from a less protected avenue. For example, a company's email gateway prevents the malicious actor's penetration attempts so the attacker will move on to target the mail servers of trusted customers, business partners, and third party providers. Gaining access to a mail server of a trusted party provides attackers a platform to launch targeted and convincing spear phishing or malware attacks with a lower likelihood of being blocked. For enterprises to extend the value of their sophisticated cyber security program, it requires a need to have deep visibility into the complete ecosystem of IT components and to understand where data resides. Full visibility includes having an understanding of the associated external connections.

Determining the effectiveness of security is difficult, because you don't know how well it works until you're attacked. To understand how the defenses are operating requires authorized simulated penetration attempts against the information systems. Penetration testing is performed to identify the strengths and weaknesses of the system. Black box penetration testing is conducted as a hacker would attack a system, using only openly available information for background. Determining the potential risks of partner and supplier operations as they relate to the enterprise should include assessments that are similar to black box pen testing.

Companies remain vulnerable to losing critical, sensitive information via a broad range of third parties either directly connected to the network or containing access to valuable assets including data. It is imperative all risks an enterprise assumes as a result of shared connectivity and data is assessed. Organizations have many options for evaluating third party providers regarding their offerings, financial health, and leadership however there is no easy method for determining the cybersecurity posture of the Third Party organization. It takes work to get it done properly.

When run as part of a Third Party Cyber Risk Management (TPCRM) process, there are a number of interconnected activities that should be performed to raise the probability a complete and accurate profile. The TPCRM process relies on two primary reviews, a policy and compliance assessment and a technical review. Using the responses to Shared Assessments' Standardized Information Gathering (SIG) questionnaire it is possible to get a good understanding of the processes and procedures associated with 18 individual security domains that include Cloud Security, Access Control, Security Policy, Incident Response, and Privacy. The questions are based on various industry standards, which include ISO, COBIT, PCI, NIST, and FFIEC. The answers to the questions tell CISOs how an organization intends to handle cyber security issues, however they can't inform you how successful they are in terms of implementation. This is where the technical assessment component comes into play.



The technical evaluation provides an attacker's view of the organization by performing passive and unobtrusive scans to develop a detailed map of a company's infrastructure and to ascertain what vulnerabilities might exist. Starting with only a domain name much information on the domain, subdomains, websites, and IP assets can be discovered. Additionally, hacker forums, paste sites, social networks can be crawled for the company and domain names. Specific areas that should be checked by third-party technical assessments include:

01 DNS scan to ensure a company's Domain Name Server has not been compromised, thus resulting in the redirection of legitimate traffic to corrupted servers.

02 Monitoring data confidentiality by ensuring that the SSL/TSL function is properly working to support secure communications between web servers and browsers

03 Email security to evaluate the Domain-based Message Authentication, Reporting & Conformance (DMARC), DomainKeys Identified Mail, (DKIM), and Sender Policy Framework (SPF) to verify that they are in use and are configured correctly

04 IP Reputation checks to see if an organization's IP Addresses have been included on any blacklists

05 Web applications and network systems need to be scanned to uncover what, in any, vulnerabilities and misconfigurations are present

06 Credential are checked against databases of known passwords and logins to see if any have been compromised

To allow consistent measurement, the Third-Party reviews should use a grading methodology that depends on well-accepted frameworks such as MITRE's Cyber Threat Susceptibility Assessment (CTSA) and Common Weakness Risk Analysis Framework (CWRAF™). To be fully effective, all of the third party assessments must be continuously updated and monitored. Working within the existing TPCRM framework provides a lot of information about the relative strengths and weaknesses of the cyber security posture of partners. However, it does not provide the financial impact on the enterprise should a third party suffer a breach. To make a calculation on financial loss, enterprises need to look at the FAIR methodology and the vendors who support its usage.

GETTING TO KNOW YOU WITH NORMSHIELD

When hackers identify their targets, they first conduct cyber reconnaissance. They quietly scan and map company internet footprints, discover cloud and web applications, collect stolen credentials, and identify critical data and assets without being noticed. Hackers then leverage open-source intelligence resources like internet-wide scanners, deep and dark web, social networks, search engines, leaked database dumps, and even legitimate security services. In order to know what attackers know about organizations with third party connections, it requires dedicated tools with potential to collect and analyze information on hundreds if not thousands of potential entities, and deliver reports that provide value to decision makers. Third-Party Cyber Risk Management tools, such as NormShield can evaluate the security capabilities of vendors.

NormShield is a Software-as-a-Service, external risk measurement tool that combines open source intelligence with a non-intrusive cyber reconnaissance platform. The platform collects a wide range of information without touching the target customer, leveraging advances in data science and machines which learn to provide higher frequency and precise real-time risk assessments. Its data collection goes deep enough to provide sufficient visibility in a timely manner. The platform can provide continuous risk monitoring of partners, keeping ratings up to date as situations on the network change. The value proposition of NormShield's 3D Vendor Risk @ ScaleSM includes construction from a practitioner's perspective, full visibility into a vendor's cyber position, and MITRE standard scoring system including FAIR to provide potential financial impact assessments.

NormShield uses the same open-source intelligence tools and techniques hackers use. They have hundreds of data collectors, crawlers, and honeypots continuously gathering information from internet-wide scanner databases, reputation sites, cyber events, hacker shares, and known vulnerability databases. The NormShield comprehensive cyber risk assessment system collects specific information about all aspect of a firm's external cybersecurity posture by capturing 288 unique items in 20 categories. Each category provides specific information about each piece of a firm's cybersecurity posture. Executives get easy to understand reports with letter-grade scores and IT security teams can drill down to the technical details in each risk category. The rating reports complement the information included in the Shared Assessments' SIG Questionnaire, which can be uploaded into the system. NormShield correlates these findings against industry standards and best practices, allowing for a compliance level of understanding.

NormShield relies on an open standard scoring system instead of having a proprietary system, often misunderstood. This mentality allows the measurements to be repeated and widely understood using the MITRE Common Weakness Scoring System and the Common Weakness Risk Assessment Framework. The framework is a mechanism for measuring risk of security errors in a way that is closely linked with the risk to an organization's business or mission.

NormShield uses the FAIR model to calculate the probable financial impact of a third-party vendor, partner or supplier experiences a breach, and communicates risks in quantitative, easy to understand business terms. Leveraging FAIR assessment at scale for TPRM helps attain the goal of cost effectively achieving and maintaining an acceptable level of loss exposure, while also clearly conveying the breadth of probable impact to the organization.

With NormShield, companies can have a three-dimensional view of the technical, compliance and financial impact of a cyberattack to better understand the full risk relationship with a partner or supplier. For some, the business benefits will outweigh the cyber risks. For others, it may not.

CONCLUSION AND RECOMMENDATIONS

To remain competitive in a fast paced and ever evolving business environment, organizations are required to exchange critical business information across network boundaries to take advantage of advanced information technologies, such as cloud, mobile, SaaS, and IoT. These transformative technologies contribute to greater productivity, also broadening the attack surface exposing an organization to new cyber threats. Enterprises have increased their cyber security efforts to strengthen internal security controls, however the growing reliance on third parties --- partners, suppliers, and cloud hosting services --- directly linked to networks has become a major concern. According to multiple surveys, up to 60% of all data breaches could be linked directly or indirectly to access given to third parties. The issue will only grow, as the reliance on external partners and resources will increase as connectivity continues to expand.

Ensuring that cyber security supports a company's business mission requires a strong risk management process that can identify the real value of security, and can be used to assess and make adjustments when technology and events change the risk posture, eliminating snap judgements. Companies have learned to limit their risk exposure by adopting a risk management strategy that identifies the risks, how those risks could impact the organization and what controls are in place to mitigate those risks. Cyber risk management has evolved, but is still well behind other risk assessment processes business executives often rely on to calculate the probable financial impact of a given risk. The Factor Analysis of Information Risk (FAIR™) is a process many organizations have begun to adopt, putting cyber risk in business and economic terms. This process can lead to better prioritization of risk and more effective allocation of resources.

An enterprise Cyber Risk Management program should look at internal security, perimeter security, data security, but also must cover an organization's overall cyber ecosystem. This perspective should include all parties either directly connected to the network, or containing access to valuable assets. What gets measured is what gets managed, requiring companies to take control of their third-party exposure and implement safeguards and processes to reduce their potential exposure. By incorporating third party risk assessment capabilities into the overall cyber security process, it's possible to extend visibility into areas normally unknown. There are a slew of options when looking at third-party cyber risk management tools, however NormShield's ability to provide technical policies and processes (analysis of the SIG Questionnaire), and financial metrics (FAIR results) is an intriguing value proposition offering up a complete picture of a vendor.