Work From Home Work From Anywhere Facts and Fiction
A Risk Based Approach

Presented by

Howard Glavin CISM, CRISC, CDPSE, QSA, CTGA, PCIP, ISO/IEC 27001
Senior Lead Auditor
Executive Vice President - K3DES LLC
howard.glavin@k3des.com
904.287.4433 Home Office
904.631.9204 Mobile
904.287.2213 FAX
Secur8ty Skype ID

WFH Facts and Fictions:

The Risk-Based Approach to Working from Home

Preface

Today, a very large portion of the working community is work from home (WFH) staff. This is in part due to the Covid-19 lockdown, but it has its roots in cost reduction, employee attraction and satisfaction and profit maximization.

Many papers and other forms of publication have been written to explain to the reader how to make WFH activity work for the employer. Some have been based on pure logistics, some have been based on cybersecurity considerations, and, frankly, some have been based on fiction.

The purpose of this paper is to discuss facts and fictions associated with WFH staffing models, and to highlight risks associated with various WFH environmental and technological options. This paper covers several considerations to identify the true risk associated with specific WFH scenarios. This analysis takes into account staff roles, type of data involved and relative values of data elements to determine impact to the company if that data is compromised, lost, or stolen.

This risk-based approach can be applied to all organizations, from the smallest companies to the largest fortune 50 companies.

History

Companies have been entertaining the WFH concept for well over two decades. Initially, it was to help retain the best or most critical workers who were under constraints that did not permit them to come into an office. This approach proved to be both functional and cost beneficial, and it resulted in more workhours by WFH employees as well as better employee satisfaction ratings.

Lines of business such as customer support, staff help desks, network support, and call centers began to see WFH as a way to reduce their overhead. Transition to the WFH format was already in progress at many organizations when the COVID-19 pandemic hit.

Although thought was given to individual employee roles, the overall risk of changing to a WFH structure was often not fully considered. How WFH staff were supposed to work, what they were expected to use for networks connections and workstations, and where they were intended to conduct the work were not adequately articulated to the employee. COVID-19 threw a monkey wrench into the work environment, and the end results thus far are confusion and misunderstandings.

WFH in Response to COVID-19 and Beyond

With the pandemic came panic for many businesses who were suddenly struggling to survive in a socially distanced world. WFH went from being a benefit for select staff members to a necessity to support client commitments and contracted Service Level Agreements (SLA's). Due to these sudden time and budget constraints, many risks associated with the WFH model were simply accepted in an effort to keep businesses functional.

Companies were forced to allow BYOD regardless of the risk, at least for a short time until more company-issued equipment could be obtained to support newly remote staff. While physical and logical security controls for company buildings had long since been implemented, necessary controls at many companies were not in place to ensure the physical and cyber security of home environments. Additionally, security awareness, and operational policy considerations were widely overlooked, and very little consideration was given to the need to update employee agreements/contracts to reflect the new WFH approach.

One major misconception is that WFH means work from *home*. Today, WFH actually means work from anywhere. It is very common to see people working from local restaurant's, parks, libraries, and other public places, rather than working from a private place of residence. This exposes company data to anyone in sight range or earshot.

A second misconception is that company data cannot be exposed when the staff are working within a private residence. This is not correct, as other residents and guests may have the opportunity to hear and/or see company data. Company privacy policies generally do not take this into consideration.

A third misconception is that WFH locations are exempt from audits or assessments, like HIPAA or PCI. Such assessments and audits view anywhere and anyone interacting with sensitive data as part of the assessment's scope. WFH environments will have to be reviewed by assessors or auditors as this constitutes a "work area". Depending on the geographic location for WFH, this may require specific permissions based on the individual's privacy rights. Most employee contracts do not cover allowing auditors to view the employee's home office or other private locations.

Last, but not the least, is the misconception that home networks are inherently secure. Whether connectivity is wired or wireless, including Bluetooth, is often not considered. Wireless in the office is heavily secured, but home networks in general have not undergone configuration changes to ensure secure connections. Couple this with the vulnerability of Bluetooth headsets, and the entire neighborhood may be part of the company network. Even if companies set up a Citrix environment for employee connections, these environments are only as secure as the weakest link. The weakest link in this WFH model depends on the employee workstation and home environment. If a workstation is exploited, then company data can be compromised. The explosion of successful Ransomware attacks today is based in part on this WFH business model.

The primary reason is the use of BYOD and the lack of configuration management and patching. BYOD in this case covers all platforms including but not limited to:

- Home Networks
- Workstations
- Tablets
- Mobile Phones

Interaction of Zero Trust, E2EE, and Data Management on the WFH Staff

Today we are seeing a great reluctance of employees that have been WFH to return to the Office. COVID-19 forced the issue and now that the time has lapsed, the employees would, for the most part, change jobs rather than return to the Office. This presents a long-term issue for every employer. Some of these issues are cost based:

- Office floor space
- Infrastructure to accommodate the office worker (Cubes, Devices, Server Rooms, Badges Guards, etc.)
- Day Care for those companies that supported this to allow for office workers to be in place
- Food Services
- Cleaning services
- Heat, light, AC, Trash removal

Some of these issues are philosophically based:

- Oversight and control of the employee
- Watching what comes into and goes out of the office
- Staff management from a working oversight

All three philosophical principles, when applied to the WFH staff, add to the difficulty of implementing and managing. Why?

The explanation is simple. As stated before, WFH is really "Work From Anywhere" Home can be the actual residence, Starbucks, McDonalds, The Biltmore, Disney World, Key West or the Cruise Liner.

When you add in the use of BYOD, you further complicate the use and enforcement of the three principles that will give you the best chance of securing your data and getting the work completed.

All WFH must use a Risk Based Approach to achieve the data protection required to allow for the reasonable protection of the company assets.

Zero Trust Simplified

Zero Trust is the simple assumption that you are not entitled to see any data or touch any device. All access is individually ***granted*** and is given for a very specific business need. You must log into each and every device and no Single Sign On (SSO) is acceptable. Additionally, your presentation for this Sign On is done in a form of nonrepudiation. This means you utilize the following for identification:

1. Unique User ID, Password, and MFA

Or

2. You use a Token based on a biometric and MFA. It is noted that the MFA can be part of the Biometric when using a device like, but not limited to, YubiKey.

E2EE

E2EE is the best tool to ensure that your data is protected wherever it is sent; both internally or externally. It also requires encryption when at rest so that only those with the specific trust can see it in the form and format that is required for them to conduct the work for which they are assigned.

This brings up a misconception on Encryption. Transparent Data Encryption (TDE) does not really protect data at rest because anyone with access to the database enters a data base with no associated encryption..

TDE is being phased out in PCI and has been removed from other regulatory places like banking and finance around the world. If you are using TDE currently and require PCI compliance, in the near future you will also need to add field, file, or column level encryption to your data set to protect the PAN data and SAD data; if you are permitted to save it.

For the WFH users this is even more critical. Do not think because you are a Citrix environment the data is not at risk. Many vulnerabilities exist and the end user is the weakest link.

Data Management

Data Management is a very unique topic in today's world. In the past organizations were very diligent in using structured data. Even denormalizing a database would cause management concerns. Today with Data Lakes, Data Diodes, and the "CLOUD" data location, form and format are like a maze. Most data managers today do not really know what data they have or where it is at any given point in time.

Add to this the ability of WFH to screen scrape, download, Snapshot, and monitors that can record the images the see, you are adding to the locations of data in your control and outside of your control.

It behooves the business today to plan where the data resides and how the data is going to be stored, monitored, audited and logged. Data is the holy grail of the business. WFH makes the location, monitoring, and care of the data even more important. Couple this with the risk of Ransomware and you have the perfect storm. All data should have at least one version as close as possible to the current volume level in a storage that is not touchable by humans and not corruptible by the use of ransomware. As stated before, the workstation is the weakest link and with WFH this device is exposed to all form of oversight, monitoring, and malicious activity.

The Risk-Based Approach to WFH

Businesses today recognize the profitability of the WFH approach. Reduced office space costs and greater productivity from staff will make WFH a common model going forward, long after the COVID-19 pandemic has ended. But what about the risks? The solution is to develop a best practice for WFH that is risk-based and designed to protect the company's assets.

For a business to correctly evaluate the risks associated with WFH staff, the flow of data must be understood. What work is being done by the staff in question? Is any of the data they handle considered company proprietary, company confidential, privacy regulated, or government regulated? Examples of such data include:

1. PCI
2. HIPAA
3. GDPR
4. CCPA
5. Individual US State regulated
6. Company Confidential or Proprietary

Additionally, the company must understand the rule of employment and constraints from each state or country where the WFH staff will be handling this data. This all starts with the employment contract that now also must cover environments where the staff can and cannot work. To fully understand this, let's look at an example:

> John is an employee of XYZ company that is based in Minot, Minnesota. John was hired 15 years ago, and the terms of his employment have not been changed since that hire date. John is a call center agent that is now a WFH staff. John regularly hears or sees HIPAA and PCI data as part of his employment.
>
> John's wife is employed by another company, and she has recently accepted a part time assignment in Toronto, Canada. To ensure this move does not adversely impact the family, they buy a motorhome to use as the residence during this assignment in Toronto, Canada.
>
> John does not see any reason to notify his company, as the motor home and the campground they are going to use has WiFi for internet connectivity, and the mobile phones used for calls are serviceable in Canada. For customer calls, John uses the Company's queue system built into the call center architecture.
>
> Several potential issues are immediately apparent:
>
> - Privacy-related data from the customer is now crossing international boundaries and is subject to certain privacy rules and regulations or may not be permitted to cross the international boundary
> - The type of network connection being used may not be secure. Controls need to be in place to secure data over open public networks

- John's wife most likely will overhear the customer data and she is not an employee of the company

To tackle these considerations, we must first go back to the initial point of contact with the staff. This is the hire contract. This contract must be reviewed, updated and acknowledged by the staff to cover issues that arise when they are processing company data outside the company workspace. Some considerations include:

- The company's right to audit the work areas being used by the WFH staff. Using the example above, that would include
  - The home
  - The mobile home
  - The public area at the campgrounds for the mobile home
  - Any other location where John will be working

- Who besides the WFH staff can see or hear the data being handled?
  - Family members
  - Third Parties

- What type of connection is being used for the connectivity
  - Wired
  - Wireless
    - WiFi
    - Satellite
    - Bluetooth
    - Other

- How to report a potential data breach without putting the job in jeopardy
  - For example, if John's wife is showing her boss the mobile home while John is entering HIPAA and other regulated data, this could lead to a data breach.

- Reporting a change in geography for WFH employees
  - Movement within the company's country
  - Movement outside the Company's country
  - Movement to Countries with high risk of riots and disruption
  - Movement to Countries that are prohibited by the Company's home country
  - Movement to Countries that require complete control of the computing equipment connecting to the internet

- Implementing constraints on WFH locations
  - Home only
  - Private areas not associated with the home
  - Public areas
    - Restaurants

        - Parks
        - Libraries
        - Airplanes
        - Cruise Ships
        - Trains
        - Other Public Transportation

- Other constraints associated with the specific company and the type of data being worked.

The next consideration is the type of equipment being used by the staff. This can be company-owned or bring your own device (BYOD).

Considerations for company-owned equipment:

- Capture of all the logging and configuration data required, based on the type of data being processed
- Privacy screens to prevent viewing from angles other than directly in front of the device
- Locking down devices so that no software installations or configuration changes can occur that are not approved by the company
- Preventing the use of split VPN Tunnels
- Implementing controls like multi-factor authentication to assist in positive identification of users
- Enabling cameras so that management can view staff during work hours, like in the workplace

Considerations for BYOD:

- Explaining to the owner of the equipment (note: this owner may not be the user of the equipment) that all data on it may be subject to search warrant or other legal requests
    - The owner of the equipment is the person who purchased it and is responsible for it.
    - For example, the head of the house buys a laptop for the home, and the employee is a member of this family. In this case, the owner is a separate individual from the WFH employee
- Who is going to replace this equipment if it is seized, lost, or stolen?
    - Has the owner of the equipment agreed to these terms?
    - How is the owner's own data going to be replaced if at all?
    - How are the applications etc., loaded on the BYOD device verified as owned by the user for accurate replacement if the company is going to replace the device?
- How to report the equipment being seized, lost, or stolen if this loss does not occur in relation to the employee's work
    - For example, a shared family laptop is seized due to illegal activity by a non-employee family member.
- What can and cannot be loaded onto the equipment

- What safeguards cannot be turned off due to the type of data being processed for the company
- Preventing the use of split VPN Tunnels
- Implementing controls like MFA to assist in positive identification of the user
- Enabling cameras so that management can view with staff during work hours, like in the workplace
- How vulnerability scanning of this equipment will be accomplished (Note: Scanning is a requirement for PCI DSS compliance)
- How this device going to be penetration tested (Note: Penetration testing is a requirement for PCI DSS compliance)
- Who is responsible for maintaining the applications on the device to ensure only supported software is in use?
- What logs are being ported to the company's log host (Note: Retaining logs in a centralized log host is a requirement for PCI DSS compliance)
    - Has the owner of this equipment agreed to these logs being ported to the company's log host?

The longer the WFH model is implemented, the more relaxed the WFH staff member becomes about how to conduct the company business.

Little things that indicate the lack of following the rules of engagement are:

1. Employees working from a more open room, like a living room or kitchen vs. the bedroom or closed area
2. Employees having friends, family, and guests in the work area during work hours, potentially exposing them to the company data
3. Employees conducting home repairs with repairmen in the same location as the employee's work activities
4. Children interacting with the employee during calls
5. Family members and others in the work area of the employee during video conferences
6. Employees working at restaurants or other public places
7. Employees using devices (headsets, speakers, etc.) that were not issued by the company for such use

Due Diligence

Most federal and municipal courts have issued a finding of gross negligence for the lack of conformance to a due diligence level of protection. Gross negligence is any level of risk acceptance that is below the threshold of due diligence. What is due diligence as applied to security risks? This is generally defined as those activities a reasonable person would require for protection for their information assets.

Because this may be difficult to understand in theory, the following example demonstrates a practical application:

Example: A group of regulated assets needs protection from non-authorized viewing or use. The value of the assets is one million dollars. This value is the fully loaded cost of ownership, including potential fines and other penalties.

The business determines that this asset does not need protection, as they do not believe the regulations are correct. They choose to put forth no effort and spend no funds in the safeguarding of the assets.

This willingness to place assets at risk could be viewed by the courts as having a lack of due diligence in the assets' protection.

Why should the business be concerned with the court's opinion? In today's litigious society, challenges brought by the private or public sector could end up in the courts for consideration and dispossession. Keep this in mind as the business creates an asset protection and risk assessment process. The process should be based on best practices and able to withstand due diligence or other challenges in court.

The Risk Assessment for WFH

The risk assessment will cover risks associated with people, processes, and technologies. A mature organization will already have a well-defined risk assessment process. For less mature organizations, a risk assessment process is outlined in ***Appendix A*** of this document. Other risk assessment methods are available from a variety of reputable organizations, such as ISO 27001.

The matrix below shows how the risk of various WFH scenarios fluctuates depending on environment, technology, and contract provisions.

Intentionally Left Blank

Complexity Risk Factor	Single Family Home only Occupant	Single Family Home many Occupants - only one WFH	Single Family Home many Occupants - all WFH	Work being done in common spaces of Residence	Work being done at Coffee Shops or Restaurants	Work being done via Company Developed and Managed WiFi Settings	Work being done via default WiFi Settings	Work being done via Company supplied Wired Headset	Work being done by Company supplied Bluetooth Headset	Work being done by BYOD PC	Work being done via BOYD Bluetooth Headset
Contract covers working in the office per the PCI DSS Requirements	20	25	25	25	25	25	25	25	25	25	25
Contract covers all PCI items for WFH	5	20	20	20	25	20	20	25	25	25	25
Contract covers only the general office work constraints	15	20	20	20	25	20	20	25	25	25	25
Contract does not cover job sharing within the family	25	25	25	25	25	25	25	25	25	25	25
Contract does permit assessment of home work area	10	10	10	10	25	10	10	25	25	25	25
Contract stipulates the device cameras is "ON" during all work hours and can be viewed by the management	5	5	5	5	25	5	5	25	25	25	25
Contract has a process for accidental data exposure for reporting to management	5	5	5	5	25	5	5	25	25	25	25
Contract does not have a process for accidental data exposure for reporting to management	25	25	25	25	25	25	25	25	25	25	25
Contract permits assessment of the Home workspace with prior notice	15	15	15	15	25	15	15	25	25	25	25
Contract does not permit assessment of home work area	25	25	25	25	25	25	25	25	25	25	25
Contract does not prohibit "family" job sharing	25	25	25	25	25	25	25	25	25	25	25

Table 1: WFH Risk Analysis Matrix

Let us examine the complexity values associated with the WFH model using a few examples:

Example 1: A call center agent who accepts credit card and HIPAA data works from a shared apartment with four roommates who do not work for the same company. The apartment has two bedrooms, and one common area. All four individuals are in WFH mode for their various companies. They all work from the kitchen table in the apartment or go to the local coffee shop with WiFi and outside dining to conduct their required work. The employee who accepts credit

card data and other privacy regulated data is using a company supplied laptop that is built to the company hardening standards but is using their own ear buds via Bluetooth connection to the laptop, as there is no mic or speaker jack.

This example creates a complexity value of 25 based on the above details for BYOD Bluetooth earbuds.

Example 2: A call center agent who accepts credit card and HIPAA information is in a single-family residence with their immediate family in the residence while they are working. While home, the employee must also ensure the children are doing their remote learning, and thus sets up the work area in the family room to be able oversee them. Additionally, other family members are engaged in similar WFH activities for other companies.

This example creates a complexity value of 25 based on the above details.

Example 3: A call center agent who accepts credit card and HIPAA information is in a single apartment as the only resident and does not have guests during work hours. They have set up their “office” in a spare bedroom behind a locked door. The employee is using the company-supplied wired headset but is using the home WiFi router with default settings. The connection to the company network is a VPN with MFA.

This complexity value is between a 10 and 20 depending on the VPN being split tunnel or no split tunnel. If the employee was using a company-supplied and configured WiFi router, this would be a complexity value of 5.

Example 4: A general support call center agent is working in an environment like example 2 above. They purchased their own wireless router. All of the default wireless settings are in place, and no encryption is being used for the connection from the headset to the workstation or phone line.

This complexity value is 25 based on how the device is interacting with in the company environment are tied back to the regulated data devices.

Example 5: A device administrator is using a company-supplied laptop through a company-supplied WiFi router and has a wired headset. They are working from their locked bedroom and ensure the device is logged off or locked when not in use.

This is a complexity value of 5.

Example 6: The company has outsourced device management and datacenter activities to a service provider, who in turn has outsourced to three other providers. The Azure cloud is being used for the data center, a local friend for the device management, and a third party for NoC and SoC activities. Due to the

COVID-19 pandemic and local regulations, all of the service providers' activities are being done via WFH staff. The company is only aware of the initial Service Provider and none of the other companies under them. It is noted the company must know all of the companies it outsources services to; if that company outsources its activity in support of the company, those third parties must also be known to the company.

This is a complexity value of 25

Suggestions

1. Implement Zero Trust, E2EE, and Data Management.
2. Obtain companywide values for the assets engaged in WFH by Roles and Responsibilities as discussed above
    a. This will give the relative cost value to use for the calculations in either actual dollars or in percentages
    b. Caution: the value cannot exceed the total value of the company, as this is a subset of the company operations
3. Divide the WFH roles into those that handle general public information and those that handle regulated and privacy-controlled data
    a. Administrators including DBAs are in the privacy and regulated data 99% of the time, since they can impact or view the regulated data.
4. Keep it as simple as possible for the initial pass. The more you bifurcate the roles, the more complex the cost value becomes, and the more difficult the complexity value becomes to calculate.

Conclusions

Whether implementing WFH activity for a short time or as permanent solution, it must be secured by the same type of controls used to control the conventional office workspace. The more deviation from these controls, the greater the risk to the business. This risk could become so great that the company could potentially fall outside due diligence and slip into gross negligence in the protection of company assets.

APPENDIX A

Risk Modeling Overview and Concepts

Creating a value for assigned asset protection requires not only the knowledge of the assets in question but also the criticalities, threats/vulnerabilities, cost of replacement, and complexity associated with the development and protection of that asset or asset group.

An action plan is the remediation and/or mitigation plan. Mitigation plans are short-term patches to reduce risk to a near-acceptable level. These plans are designed to meet the minimal due diligence level of risk acceptance. It is critical to understand that mitigation plans do not determine root cause. However, mitigation plans do address root effects in the narrowest of terms. A remediation plan addresses the root cause. Some assets may have a short-term mitigation plan followed by a full remediation plan.

Determining root cause will be crucial for the remediation plan. The root effects depicted by asset vulnerabilities will have a many-to-one relationship to root cause. If the effects have a one-to-one relationship to the purported root cause, this indicates that the business has not determined the true root cause. Generally, this finding of a one-to-one relationship exists when silo-structured organizations only look at the vulnerabilities in their silo. This can also occur when Information Technology attempts to remediate without the input or assistance of the business. All businesses today in both the public and private sectors are interdependent with all the other areas of that business.

Developing a Fully Loaded Risk Factor (FLRF)

The steps to determine FLRF is as follows:

1. Group assets into similar types and/or granularities
2. Determine the fully loaded risk factor (FLRF) for that asset or asset group
3. Develop the rank ordering of low to high of the FLRF
4. Develop the rank order form low to high of the FLRF for all medium risks
5. Determine the lower limits of acceptable risk so that a viable business risk can be acceptable but also documented
6. Determine the upper limits of acceptable risk
7. Develop a mitigation plan for all assets determined to be at unacceptable risk levels
8. Determine potential root causes and validate by testing
9. Develop the remediation plan to address the root cause per asset or asset group by risk ranking from the FLRF
10. Develop the metrics for successful completion of each step or phase of the remediation plan
11. Test the plan for at least one asset, and adjust the plan as needed to meet requirements of solving root cause
12. Turn remediation plan over to Information Technology for ownership

The process is very straightforward, but it is necessary to discuss the underlying logic to understand this activity. This process is both science and art in that it requires opinion as well as subjective and objective reasoning. Blindly following the process in developing the remediation plan will lead to failures, as each step has predecessors and descendent dependencies.

Asset Grouping

The process of grouping assets into common groups allows for even granularity across the business from the assessment findings, thus creating the best chance of determining root cause. The WFH asset will have one asset group and the value of this group will vary depending on the function being done by the specific WFH staff.

The value of this “Work Group” is generally determined by the finance department.

Examples of these asset groups are:

1. Call center agents that work with financial records, credit cards, or other privacy regulated data
2. Call center agents that support general needs with no access to privacy-regulated records
3. General support agents that can establish or reestablish the customers’ connectivity
4. General support agents that can only answer general questions and have no ability to see customer data
5. Server or network administrators
6. Database administrators
7. Human resources
8. Service providers that are supporting the business activities on behalf of the company
    a. Examples
        i. Call center customer support for payments or dealing with regulated or privacy related data
        ii. Call center general support with no access to regulated or privacy related data
        iii. Server, network, or database support
        iv. Cloud services

All the above WFH staff have a different risk associated with the roles and activities they fulfill. When the activities are through a third party, the risk is more complex and is generally tied to contract language.

Determination of the Fully Loaded Risk Factor (FLRF)

The process to determine this factor is developed from the following calculation:

*Formula 1: (V) * (R) * (C) = FLRF*

- Vulnerability/Threat is set as **V**
- Complexity Value is **R**
- Criticality is set as **C**

To arrive at the value associate in Formula 1, the business must use the derivations for each of the values in the formula from the logical and physical groupings.

Vulnerability/Threat (V) – The vulnerability/threat factor is derived from averaging the individual risk values for the assets in the group. The assessor assigns these values as high, medium, and low. The numerical representation for high is a positive 5, medium is a positive 3 and low is a positive 1. Add all the values and divide by the total number of objects. Then round up to the next positive whole integer. The lowest value for this variable will be positive 1 and the highest will be positive 5 based on the rounding.

Complexity Value (R) – This value refers to the difficulty an asset or group of assets will present to the task of addressing root cause. The initial review will look at the set of root effects and place the potential root cause.

The business will tag and evaluate this initial root cause to determine if it is behavior or activity-based. If it is activity-based, it will be set aside and reworked until the business can place a specific behavior or lack thereof as the causing factor. The business will then tag this finding as the root cause of these actions.

Set the value of complexity in a range of positive whole integers of positive 5, 10, 15, 20 and 25, with 25 being the highest complexity.

Complexity values have two roles in risk modeling. The first is to determine the FLRF, and the second is to analyze when or if the business can or should remediate the determined risk. Note that the business cannot remove all risk and sustain business. The sheer fact that the company is conducting business implies some risk acceptance.

Criticality (C) – The business will obtain the criticality factor in part by the assessment activities, with the individual asset owners ranking each listed asset from a value of 1 to 5. The value of 1 is low and the value of 5 is High. As the individual asset values are obtained, they will be grouped into logical groups driven by the senior team and the CFO to ensure each grouping is of like size or importance to the company. Dissimilar sizing will lead to skewed values. Typical criticality groups are Applications, Data, Infrastructure (Owned or Leased), Good Faith Value, and Staff. Part of this valuation will be averaging received ratings and rounding up to the next whole positive integer. The acceptable values for criticality will be from 1 to 5.

As part of the criticality factor, the business will use the value of the assets. The value determined in the criticality assessment also known as Total Cost of Ownership (TCO) or simply Cost. Use this cost value in determining risk to apply the value of the asset or

group of assets (z- axis) to the vulnerability (y-axis) and criticality (x-axis) for graphical representation.

In the area of risk and risk management, the graph formed by these values starts at the coordinate (0,0,0), or root of the graph, and moves up and out in a parabolic curve that will reach vertical at a given point. This vertical point of the graph is where all value rises equally to infinity and any additional changes to increase the values have no effect on the slope of the graph. In the business world, this area of vertical rise is known as the point of diminished returns.

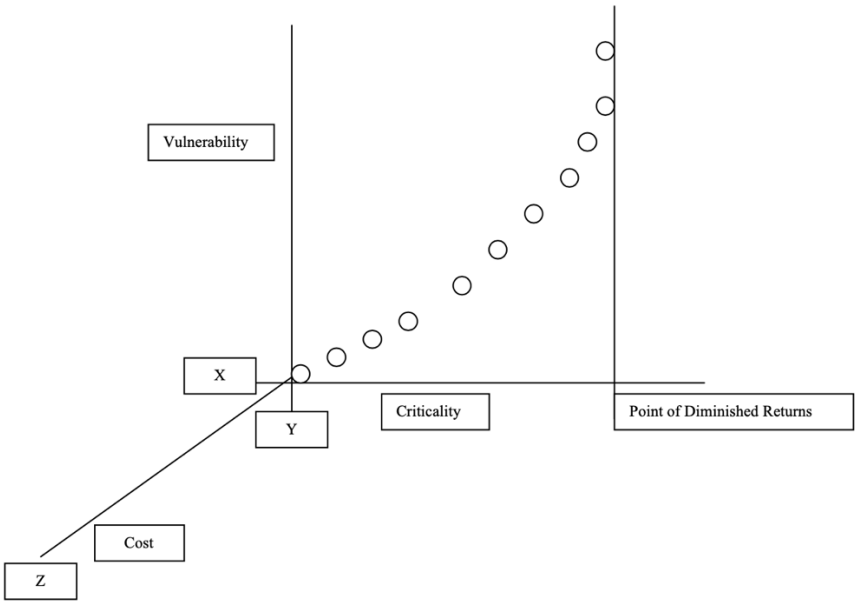
In evaluating the risks to an asset, the business must consider that exposing the asset, or group of assets, to fines or other actions could cause loss or economic impact to the organization. It is possible for the potential loss caused by an asset valued at $100,000 to exceed the full value of the company and its tangible assets. Although there is only a remote possibility that this would occur, if a court were to find grossly negligent behavior, it could impact such fines.

For the purposes of this risk ranking, and to place a full exposure limit on these assets or groups of assets, we will set the full exposure limit to the total value of the company as reported in the last annual report. Factually, this could include the value of all tangible property owned. This value can be either dollars or percentages but cannot be a mix of each. Additionally, the cost totals must add up to the 100% value of the company be it the book value or imputed value used for all accounting tax purposes.

For this discussion we need to explore the value and evaluation of the analysis vector of Cost. For this purpose, cost can be equated to value to the company. This value covers the people, processes, and technology in use. Generally, this value is first broken down by role and responsibility. Examples are administrators, internal support staff, external support staff, call center agents with access to privacy regulated data, call center agents with access to only general information that is deemed public by the company, and third-party support companies fulfilling any of the above roles.

The finance department must be involved in determination of the “Cost – Value” of the assets, as they are the only department that has the full picture of the company’s value, both overall and by asset. Other departments may have less subjectivity and place unrealistically high values on their own assets.

Figure 1.0 Vulnerability, Criticality, and Cost Graph



The three Axis are:

1. X axis Criticality
2. Y axis Vulnerability
3. Z axis Cost

We will use all three values – vulnerability, criticality and cost – to determine the upper and lower limits of acceptable risk.

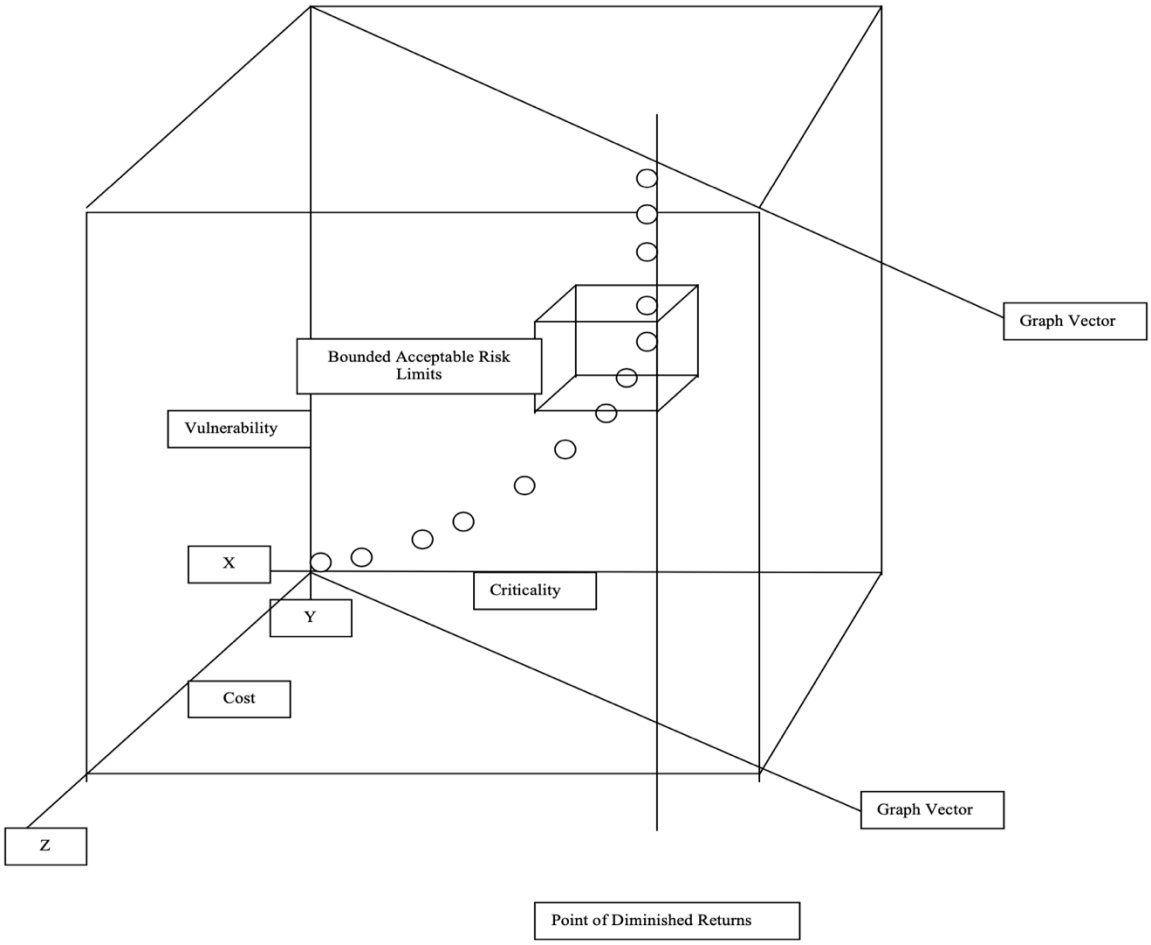
Theoretically, this range has a lower limit bounded by the area where taking additional risk would result in a finding of lack of due diligence or gross negligence. The upper limit of this range is bound where the additional input of risk mitigation adds no additional value. The point of diminished returns graphically depicts this theoretical point.

The cube shown in Figure 2.0 below shows these bounds for both the value add and the loss of value areas. All activity to the outside of the curve is negative activity as it adds cost, etc. without adding value to the protection of the asset or group of assets.

The size of the cube does not represent any logical bound (as shown in the Figure 2.0) and is used only to show that a range occurs. The actual upper limit of the range is the point of diminished returns. The lower limit is that which is determined by the company to be excessive risk. As confidence and modeling ability grows in the risk areas, the business's ability to tune this upper limit will become much easier. The value able to push this upper limit down and keep it inside reasonable risk reduces the cost of asset protection, and thus more profits are available to apply to the business. This tuning

process of risk acceptance allows for an ROI or cost-to-benefit ratio that is favorable and shows good business practices and decisions.

Figure 2.0-Bounded Activity Area of Acceptable Risk Graph



When an acceptable risk limit is not available from which to start analysis, the business needs to create one. A general rule of thumb is to apply the 80/20 rule for asset protection as a starting point.

Point of Diminished Returns requires 80 percent of the asset protection value to be utilized. This artificial starting point can then be tuned to achieve true business-based risk model boundaries.

Use caution when introducing new assets or asset groups to this risk range to allow for full validation of the accuracy of the range.

Fully Loaded Risk Factor (FLRF) – At this juncture, the business can now calculate the fully loaded risk factor. To determine this factor for each asset or groups of assets, use the following mathematical formula:

(V) * (R) * (C) = FLRF

Now that we understand the basics, we can apply this knowledge to fully understand the companies risk factors as they apply to the WFH activities.

The formula and calculations are simple. However, applying the discipline and rigors to arrive at the required values is a little more arduous.