Method to Identify High Value Assets for Small Government Agencies and Small to Mid-sized Organizations

Natalie Sjelin
UTSA CIAS
Natalie.Sjelin@utsa.edu

Glenn Dietrich Ph.D.
UTSA COB
Glenn.Dietrich@utsa.edu

Abstract

In today's increasingly connected world, it is more important than ever to ensure an organization's information and information systems are protected from cyber threats. Every organization has critical information and technology assets that are essential to their business operations and require enhanced security. Organizational resources that can be dedicated to cybersecurity are finite; therefore, those resources should be applied deliberately and strategically focusing on the most important assets. While large cities, states and corporations, with robust IT capabilities, may be able to align their processes with federally mandated directives to identify those critical assets also deemed high value assets, the smaller government agencies and small to mid-sized organizations require a scalable and flexible process based on their individual requirements. This paper will describe a method for identifying high value assets that can be integrated into an organization's or agency's cybersecurity program.

1. Introduction

The cyber security landscape has changed from the "script kiddies" of a few years ago to the well-organized professional actors of today. The script kiddies were most interested in displaying their skills and accomplishments by hacking into a business firm or a government agency and then bragging about their accomplishments. The actors of today represent professional hacking groups and or nation states that have goals of political turmoil or financial gain. For example, China and Russia have been the leading cyber security bad actors for the last 15 years. Research conducted from the Center for Strategic and International Studies examined publicly available data on cyber-espionage and cyberwar focused on cyber-attacks on government agencies, defense and high tech companies or economic crimes with losses of more than a million dollars. The study reveals from 2006 to 2018, China was involved in 108 cyber incidents with losses of more than $1 million each. Russia has been responsible for 98 major cyber incidents with losses of more than $1 million each. Next in the ranking came Iran with 44 incidents, and North Korea with 38. India was listed as guilty of 16 important cyber incidents from 2006 to 2018, while the U.S. was accused of nine. The rest of the world had 67 incidents [1]. According to Cybersecurity Ventures, the damage related to cybercrime is projected to hit $6 trillion annually by 2021 and cyber security spending is expected to exceed $1 trillion.

Much of the increase in hacking is because of the advances in technology in the areas of software development and communications. The capabilities of the software that is used in the hacking has become more sophisticated and more available on the Internet. The AV-TEST Institute has identified an average of 12 million new malware routines each month for the last year. Each of these malware routines has variants and thus compounds the difficulty in defending the cyber systems. The basic ransomware platform that was used in the recent pipeline and meatpacking exploits is available for purchase on line. Open source software tools provide the arsenal for the nation states and other gangs to threaten the extortion of business and government entities [2]. Many of the tools are updated regularly so that they remain effective to changes in the cyber security landscape. Cybersecurity Ventures estimates that ransomware attacks a business every 14 seconds. According to the Accenture Report "The biggest takeaway from our research is that organizations should expect cybercriminals to become more brazen as the potential opportunities and pay-outs from these campaigns climb to the stratosphere." Ransomware has become the new business model for cyber criminals.

Ransomware has several methods for achieving the desired result. All lead to extortion or loss for business systems. The malware may be used to steal data such as financial information that can be sold on

URI: https://hdl.handle.net/10125/79616
978-0-9981331-5-7

the black market or used for identity theft. Software is frequently used to encrypt data files that can be returned to normal only after a ransom is paid and an encryption key is provided. The data threat may be to make confidential data public, embarrassing someone in particular, which could become a political situation. It may be used to steal credentials that can be used to sign on to other systems. Frequently, the malware is used to attack the business systems. However, attacks can also be targeted to industrial control systems such as the electric grid or a petroleum distillation tower. Regardless of the target, they all have the same message; pay or suffer the consequences.

With the current computing and communication technology, it is not possible to have a system that cannot be hacked. Systems have to be designed so that they are resilient and important functional assets are well protected. This protection process begins with determining the value of system components and functions.

High Value Assets (HVAs) is the term that describes critical assets that support a community's or organization's mission or critical operations, including critical information that is processed, stored, or transmitted. These assets, systems, and datasets may contain sensitive controls, or data making them of high interest to criminal, politically motivated or state-sponsored actors. These malicious actors may be particularly interested in targeting these assets for direct exploitation of data or to cause a loss of confidence by the public. Adapting a strategy to assist a community and the organizations within it to identify and prioritize high value assets will enable them to dedicate people and financial resources to those assets ensuring better security and resiliency of HVAs.

2. Traditional Methods to Value Assets

Organizations have been using valuation methods since the early 1900's to determine the value of the business. In the 1960's valuating assets emerged to improve business decisions. Asset valuation is a process to determine the value of tangible and intangible assets. Common methods of asset valuation include the Cost Method, Market Value Method and Standard Cost Method [3]. The cost method is based on the value of the historical price when the asset was purchased. This method is used to recognize the asset in inventory and fixed asset accounting. The market value method is based on the value of the asset on the market or the projected price when sold. This method is helpful when determining a replacement value for an insured asset. The third common method used is the standard cost method which uses expected costs instead of actual costs. This method is done by obtaining the recording differences between expected and actual costs. The standard cost method is generally used to measure cost control and performance to assist in determining profit margins based on projected costs [4]. There are many reasons to value organizational assets such as identifying the right price for an asset to ensure the organization does not overpay; to determine the value of the business; to determine collateral when a company applies for a loan; and verifying the value of assets as part of an audit. While each of these methods have useful purposes, none of them have a risk management approach that would apply to cybersecurity.

3. Federal Directives and HVA Approach

The Federal HVA Program initiative was established in 2015 through a directive from the Office of Management and Budgets (OMB). OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) directs the Federal Civilian Government to strengthen their cybersecurity through five objectives. One of the objectives requires agencies to have prioritized identification and protection of high value information and assets, resulting in the HVA Program [5].

December 2016, OMB Memorandum M-17-09 defines HVA in a single definition and is updated in December 2018 through OMB Memorandum M-19-03 to provide flexibility by adding multiple categories under which an agency may designate an HVA. The categories defined for identifying critical assets are:

- Informational Value – the information or information system that processes, stores, or transmits the information is of high value to the government or its adversaries
- Mission Essential – the agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEFs) as approved in accordance with PPD-40 National Continuity Policy, within expected timelines without the information or information system
- Federal Civilian Enterprise Essential (FCEE) – the information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

Federal Information Processing Standards Publication 199 (FIPS PUB 199), February 2004,

defines the security categories for both information and information systems and defines three levels of potential impact (low, moderate, high) on organizations or individuals if a security breach were to occur [6]. The context of the impact must take place within the organization and pertains to the overall national interest. The potential impacts are defined as follows:

- Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, operational assets, or individuals.
- High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The federal directives are focused on national security to include protecting national resources, the economy, citizens and institutions. The established Federal HVA Program cannot be applied directly to non-federal organizations. Although, many of the directives could be used as guiding principles for a HVA program, a new program must be developed that is flexible and scalable enough to be implemented by State, Local, Tribe and Territory (SLTT) jurisdictions based on their individual requirements and can be modeled from the Federal Government's HVA Program. Additionally, small to mid-sized organizations would also benefit and could use this modified approach.

4. HVA Model Criteria

The development and implementation of a model will provide a step by step approach allowing all organizations no matter their size, extent of their resources or maturity in cybersecurity to improve their efforts to identify and protect high value assets critical to the organization. Defining the state of the organizations that will use this model is needed to identify areas of consideration to establish criteria to craft the model.

4.1 Defining the SLTT Landscape

Research conducted to establish criteria included gathering and reviewing documentation describing the SLTT landscape and interviews with SLTT organizations. The purpose of the research was to gather information regarding Information Technology (IT) capabilities associated with HVAs, to identify terminology, tools, best practices and lessons learned that may exist.

Research documentation included published reports, studies, articles, and reviews focused on the SLTT landscape associated with IT capabilities and resources, asset management practices, risk management processes and other characteristics that support an overall understanding of SLTT capabilities. The documents included in this review are as follows:

- 2020 Deloitte-National Association of State Chief Information Officers (NASCIO) Cyber Security study
- Nationwide Cybersecurity Review (NCSR) 2019 published by the Multi State-Information Sharing and Analysis Center (MS-ISAC)
- 2020 National Preparedness Report published by the Department of Homeland Security (DHS)
- 2019 National Preparedness Report published by DHS
- Cybersecurity 2016 Survey by the International City/County Management Association (ICMA)

Eight interviews were conducted from November 2020 – February 2021. The interviews were a mix of state, local and critical infrastructure entities. The organizations interviewed also represented urban and rural localities. The backgrounds of the interviewees were both technical and non-technical.

The SLTT ecosystem includes or may encompass State, Local, Tribe and Territory governments, as well as critical infrastructure and industry partners, which include small businesses, public-private partnerships, and other entities. Other entities include organizations such as independent school districts (ISDs), community colleges, or universities.

Many SLTT entities are interconnected and there is a growing concern that cyber-attacks targeting smaller public entities put state assets at risk. A 2020 Deloitte-NASCIO Cyber Security study found that "smaller public entities—such as counties, cities, towns, and educational institutions—may be particularly vulnerable ... 40% of Chief Information Security Officers (CISOs) said they feel only somewhat confident that their state assets are adequately protected from cyberattacks targeting local government." [7]

4.2 Governance Structures

SLTT governance structures broadly fall into three categories: centralized, decentralized, and hybrid structures as shown in Figure 1. These structures may vary even within a particular SLTT entity. In a 2019 survey of SLTT entities, over 95% of states and 75% of localities identified as having centralized or hybrid governance structures. [8]

Participation volume of centralized, decentralized, or hybrid governance structures within the Local peer group. Data collected in analyzing the 2,523 local organizations that participated in the 2019 NCSR.

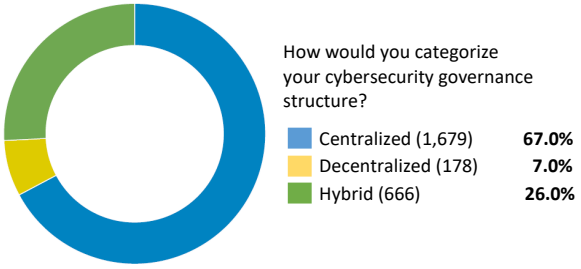


Figure 1. Governance Structures, 2019 Nationwide Cybersecurity Summary Report

Interviewed cities and states having decentralized and hybrid governance structures expressed one of the challenges they encounter is that there are some stakeholders who would need to voluntarily participate in certain initiatives such as an HVA program. As an example, the mayor of a city may not have direct authority over some county officials to discuss IT assets. At the state level, each agency assesses and implements their own asset management practices and are not required to report high value assets to the state.

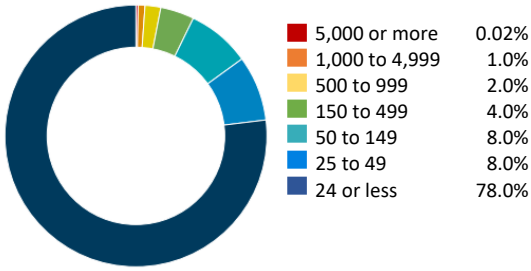
Criteria Observation #1 – the model must include guidance or an introduction that explains why an HVA Program is important and how it can assist any community to improve their cybersecurity posture by protecting their most critical information and information systems.

4.3 Resources

Resources refer to the people, money, and existing assets of an organization. The resources available and allocated by SLTTs varies widely. Through the interviews, each organization reinforced resources are limited. The IT, security and risk management capabilities varied tremendously across the interviewed organizations. The range spanned from one rural organization having no IT capabilities to states with considerably more resources but still not enough to do everything they would like to do.

Various reports describe IT and security capabilities in the SLTT community. The 2019 Nationwide Cybersecurity Review (NCSR) utilizes a maturity scale that assesses how an organization is addressing the different activities within the NIST Cybersecurity Framework (CSF). According to the report, larger organizations have a greater IT capability and tend to score higher when implementing the NIST CSF. Figure 2 states that organizations with 25 or more IT employees score 19%, however the chart also shows that only 22% of the participants have that level of staffing.

Summary of IT full-time employee staffing for NCSR participating organizations. Data collected in analyzing the number of IT staff within an organization. This data reflects all 3,135 participants of the 2019 NCSR.



- Organizations with 25 or more IT employees score 19% higher than organizations with less than 25 IT employees

Figure 2. IT Full-time Employee Staffing, 2019 Nationwide Cybersecurity Summary Report

Another key point from the NCSR is, "Dedicated security staffing also correlates to higher maturity scores." 78% of NCSR participants reported their organizations have less than five full-time security employees. With a lack in security staffing, it is difficult to begin assessing and implementing an appropriate cybersecurity program.

A survey from the International City/County Management Association (ICMA) found that less than 1% of local governments have a dedicated cybersecurity department or unit [9].

Challenges identified through the interviews reflected several insights that must be considered in the development of the model:

- **Time:** Personnel in small organizations wear multiple hats and should consider the amount of time needed for the HVA Program. Larger organizations will have more assets and will need to dedicate more time to the program.
- **Personnel:** Minimal personnel, in some cases there are no personnel, dedicated to

information technology, risk management, and cybersecurity efforts. Training for personnel is needed but cannot cost much.
- **Budget:** A high area of concern and creative measures are often taken to find funding for IT enhancements such as not hiring unfilled positions to redirect funds for IT projects.

Criteria Observation #2 – the model must include no and low cost solutions for implementation.
Criteria Observation #3 - the model must be easy to understand for personnel with any level of IT maturity
Criteria Observation #4 – implementation must have a flexible time period.
Criteria Observation #5 – functions should be described (tasks that need to be accomplished) rather than roles as there may be limited personnel to accomplish the objectives.

4.4 Existing HVA Program Elements

Some elements needed for identification of HVAs may exist in established organizational plans; however, the DHS 2020 National Preparedness Report indicates that 74% of communities reported gaps in planning and updating cybersecurity plans, and 76% identified updating cybersecurity plans as an area of high priority. Another consideration referenced in this report is a large portion of cyber infrastructure in communities is owned and managed by the private sector, highlighting the dependency of this capability on strong stakeholder relationships—a functionality that challenges many communities in the nation. Communities also reported that they have relatively low confidence in their assessment of their current cybersecurity capabilities. Therefore, communities appear to recognize cyberattacks as a concerning threat, but they may not fully understand their cybersecurity capabilities [10].

Insights from the interviews that should be considered in the model are as follows:

- **No cyber integration:**
  - Some of the SLTT organizations have risk management programs on the physical side but have not integrated cyber into it.
  - Disaster recovery, continuity and incident response plans are way behind regarding the integration of cyber.
- **HVA elements:**
  - Aspects of the HVA may be included in the organizations Information Security Policy or Risk Management and existing processes.
- **Education/Awareness needed:**
  - The business/system owners are responsible for categorizing assets and assigning them in the system of record. Most do not have a technical background.
  - Executive leadership and system owners may not really understand risk management.
- **Process involves multiple entities:**
  - Information security is under the compliance department rather than IT.

Criteria Observation #6 – a review of existing policies, procedures and plans for specific HVA related elements should be included to assist in identifying potential HVAs.
Criteria Observation #7 – a compelling introduction should be developed and shared with nontechnical system owners and leadership describing the value proposition of including the HVA methodology into a cybersecurity program.
Criteria Observation #8 – tools, templates and checklists should be included to simplify the overall process as much as possible.

5. Method for Identifying HVAs

Federal agencies are primarily responsible for designating their HVAs, however, DHS may also designate HVAs for an agency if the asset has the potential to impact national security. OMB M-19-03 directs each federal organization to report their non-national security HVAs to DHS. The SLTT organizations interviewed, indicated that organizations within a state are individually responsible for the management and protection of their assets and are not required to report HVAs to the state. State coordination is primarily voluntary. As stated previously, organizations often include non-technical business/system owners for categorizing assets and assigning them in the system of record. This makes it increasingly important for organizations to understand the need to identify HVAs and to have an easy to use method for identifying critical assets.

Every organization has high value assets that require additional protective measures. A core activity in securing the organization's environment is to identify and prioritize these high value assets. The first step is to determine if an asset is of high value. Described here are three primary areas that can be assessed as directed by OMB M-19-03 [11].

1) Informational Value - any information or other asset that has great value to the organization or its competitors.
2) Mission Essential Functions (MEFs) – the information and information systems associated with the organizations mission. MEFs are those assets if unavailable, modified, corrupted or exposed would have a significant impact on the organization's ability to offer its services or complete its mission.
3) Protective assets – those assets used for security or resilience. Security and resilience are not the same. Security assets are needed to protect the organization from attacks and breaches while resilience focuses on continuing business operations even after an attack has occurred.

Overall, an asset should be considered of high value if it has the potential to have an enterprise-wide impact. This includes cross functional processes such as operations and compliance. Reputational damage should also be considered.

The most important concept here is for the organization to recognize identifying HVAs is the activity of locating the organization's most critical information and information systems that are associated with their business mission and their ability to provide organizational security and resiliency.

5.1 Mission Essential Functions

The first step in identifying HVAs is to analyze the organization's mission and to determine what services and functions are essential. Essential services/functions are the highest priority for an organization to maintain, with minimal disruption, during all incidents or emergencies. A critical function is a service or a collection of services, normally performed by a business unit, that must continue at an acceptable level and without interruption; or the service must restart within a given timeframe after a disruption. An essential service or function will meet at least one of the following conditions:

- **Health and safety –** A service that when not delivered, creates an impact on health and safety of individuals; preserves life, prevents injury, or protects property.
- **Business failure –** A service that may lead to failure of a business unit if activities are not performed within a specific time period.
- **Required by law –** A service that must be performed to satisfy regulatory requirements; is required by law or a regulatory authority.
- **Significant impacts –** A service, if not performed, will significantly impact the business, its customers or partners. The impact may be immediate or may occur over a period of time.
- **Critical activities with downtime constraints** - Critical activities that cannot cease; activities that must be continued under all circumstances or cannot suffer a significant interruption; activities that must resume within a very limited amount of downtime.
- **Driven by mission** - Activities are driven by mission and are identified through a business process.
- **Supports critical functions** - Provides indispensable support for provision of other critical functions.
- **Vital support to others** - Provides vital support to another department, unit, or organization (with critical functions).
- **Financial** - A system that is connected to a major revenue source.

There are many important and necessary functions, but this does not make them essential. A review of the identified functions should be done to determine if it is essential to the business. One way to make the distinction between essential or non-essential is to determine if the function is necessary during a disruption and must continue during emergencies. Essential functions are both important and urgent. Functions that can be deferred until after an emergency should be considered as non-essential.

Another way to identify MEFs is to leverage work that has already been done in the organization and documented. As an example, organizations that have completed a continuity plan may have already identified some or all of the essential functions that have the potential to negatively impact the business due to an emergency, incident or disruption. Other organizational documents that may identify MEFs are:

- Business Continuity Plan (BCP)
- Continuity of Operations Plan (COOP)
- Disaster Recovery Plan (DRP)
- Memorandum(s) of Understanding (MOUs)
- Service Level Agreements (SLAs)
- Audit reports
- Contracts

DHS published a list of validated primary mission essential functions by federal department or agency such as DHS, Department of Defense (DOD), Department of Justice (DOJ), Department of Transportation (DOT), and Health and Human Services (HHS) to name a few [12]. Some of the essential functions listed include:

- DHS – Screen and secure the borders; Protect critical infrastructure, Enforce Homeland Security laws
- DOD – Formulate national defense policy; Protect and defend the country; Conduct domestic emergency response
- DOJ – Advise and represent the President, Protect Senior Officials and the Courts, Fight Terrorism and Espionage
- DOT – Assure defense transportation infrastructure; Respond to transportation disruptions; Operate national airspace systems
- HHS – Monitor and respond to health challenges; Oversee safety of medical products; Provide medical care and services

Many of the federal essential function examples do not apply to non-federal organizations. However, some of them can be modified to better reflect essential functions that may be found in SLTT and private organizations. A third approach to identifying essential functions is for organizations to review their mission and match relevant essential functions from this modified list. Additional functions may be added or those that don't precisely match can be modified. The modified list of essential functions includes:

- **Manage Finances:** Manage the organization's finances enabling continual operation of essential services and sustaining public confidence in the organization's ability to meet financial obligations. These may include but are not limited to disbursement of payments, collection of receipts, financial obligations and activities.
- **Emergency Response:** Provide emergency response capabilities. SLTT response may include law enforcement, fire, medical, and search and rescue services.
- **Maintain Situational Awareness:** Provide strategic-level situational awareness, information sharing, and decision support to leadership at all levels of government for incidents (all threats and all hazards).
- **Coordinate Continuity and Incident Response:** Coordinate continuity capabilities and manage implementation of incident response efforts.
- **Maintain Operational Communications:** Ensure the continuity of operations and reconstitution of critical electronic communications systems and services.
- **Monitor and Respond to Health Challenges:** Prepare for, mitigate, respond to, and recover from public health and medical emergencies.
- **Protect Critical Infrastructure:** Provide security, reduce vulnerability, and ensure resilience of the Nation's critical infrastructure and cyberspace from terrorism, criminal activity, and environmental hazards to ensure the delivery of essential services and functions.
- **Secure Sensitive Information:** Ensure sensitive information such as PII, PHI, PCII, Law Enforcement/Investigative Information, and other sensitive data is available to those who require access and protected from unauthorized disclosure or modification.
- **Support other Critical Functions:** Identify, protect and manage information and information systems required for another agency or organization's mission essential function. This pertains to organization's who have an essential function that is based on requests or assistance needed from others. An example would be an organization whose mission is to coordinate emergency actions after a disaster. This coordination doesn't occur unless a request and information of what is needed is provided.

5.2 Critical Assets

Critical assets as mentioned previously, can also be any information or other asset that has great value to the organization, its competitors or adversaries. This may include but is not limited to:

- Trade secrets, patents, copyrights
- Financial data
- Customer data
- Sales information
- Human resource information
- Proprietary software
- Scientific research
- Schematics
- Internal processes [13]

Other assets that may be considered HVAs include those critical assets that may impact confidentiality integrity, and/or availability, and those

assets that provide security and/or resilience to the organization. In addition, interconnections and dependencies must be documented to recognize the relationships between systems. A system that by itself may not be initially identified as an HVA, may be designated an HVA if the system is connected to or facilitates the operations of significantly important subsystems that can impact an HVA and its ability to perform a mission [14].

Existing documents in the organization that may assist in identifying these critical assets may include:

- Business Impact Analysis (BIA)
- Risk Assessment Report
- Risk Impact Assessment
- Risk Register
- System Security Plan (SSP)
- Security-related policies
- Network Diagrams
- Data Flow Diagrams
- Plan of Action & Milestones (POA&M)

6. Determining HVAs

The process for identifying HVAs may involve system owners throughout the organization who may be nontechnical. These system owners will likely be focused on identifying assets that are most critical for their role within the organization rather than evaluating the HVA as a critical asset for the overall organization. In addition, the criteria observations listed earlier must be considered, recognizing the model must take into consideration organizations that may have limited or no IT capability and the process should be easy enough to implement no matter the IT maturity level of the staff completing this step. These considerations can be addressed by developing a criterion for identifying an HVA based on the MEFs and critical assets. The criteria will assist system owners to evaluate the MEF and critical asset found in their area and apply a standardized method to assess its importance to the overall organization and to identify dependencies and interdependencies that may exist. Prior threat assessments, risk assessments or audits could be used for the development of the criterion.

A rationale should then be developed and implemented based on the unique requirements of the organization. The rationale is applied to each HVA to determine a finalized list of HVAs that may impact the ability of the organization to accomplish its mission. The tailored rationale may include continuity considerations specific to the organization such as:

- If access was lost, which assets or functions would generate the most inquiries in regard to when it will be reinstated?
- How long can this asset be unavailable before it negatively impacts the organization's ability to provide services or functions?
- Based on the total number of personally identifiable information (PII) records the organization has, how many records does this asset store or process?
- Based on threats to confidentiality, integrity and availability for this asset, what is the level of impact on the organization in the event of a compromise?
- If this system or asset was compromised, would it adversely impact a mission essential function?
- How many mission essential functions does this asset support?

7. Prioritizing HVAs

Once a comprehensive inventory list of HVAs is documented for the organization, a process to prioritize the HVAs will be needed. The method used for this initiative will be focused on scoring the HVAs to identify the most critically important asset where compromise would have the most damaging impacts to the organization. Multiple scoring factors should be included in determining the highest value assets. The following are potential factors that could be used or modified:

- **Data Type –** is the data processed or stored by this HVA of interest to a malicious actor or competitor.
- **Sensitivity of Data –** what level of sensitivity is the data processed or stored by this HVA
  - Level 0 - Available to the Public
  - Level 1 – Organization Confidential
  - Level 2 – Legal/Compliance Sensitive
- **Data Volume –** what percentage of the organizational data is processed or stored by this HVA
  - 0 – 25%
  - 26 – 50%
  - 51 – 75%
  - 76 – 100%
- **Interconnections –** how many systems/assets support this HVA
- **Dependencies** – how many internal HVAs are supported by this HVA
- **External Dependencies** – are there external system dependencies associated with this HVA

- **Other Considerations** - are there other considerations the organization may have to rank this HVA higher

Answering each of these questions, and/or other questions the organization develops, with a numbering scheme or value, as shown above, will provide a standardized method for the organization to prioritize all HVAs within the organization. This prioritized inventory of HVAs is the first step to enable the organization to know which assets are of the highest value and should have additional protections.

The time allotted for this process should be flexible as indicated in the criteria observations. There needs to be ample time to go through the process but not too much time where the initiative can lose its momentum to competing priorities. Allocating 30 – 45 days, based on the organization's schedule, allows time for the system owners to go through the process to identify HVAs in their respective areas and return a list of HVAs to a designated HVA program coordinator or point of contact. The HVA coordinator can then reconcile the identified HVAs received from each system owner and compile a comprehensive list of HVAs that are then prioritized creating an inventory of HVAs for the organization.

8. Next Steps

At the completion of this process, the organization's high value assets have been:

1) Identified
2) Examined from the organization's perspective and interests
3) Reviewed for potential threats from a competitor or adversary
4) Prioritized
5) Inventoried

This model enables the organization to clearly understand the risks associated with their most critical assets. Incorporating the HVA identification method, provides the organization with tangible and actionable information they can use to make more informed decisions and can create an action plan to better secure and protect those assets. While this model is beneficial for all organizations, the model can serve the smaller communities and agencies by providing them with steps that can increase their overall awareness of their assets and assist them in developing a plan that is flexible enough to allow them to scale improvements within their budgets and can be accomplished with minimal personnel.

The next steps for the organization are to assess the security that is already implemented for each HVA and to determine what additional controls should be integrated. There are several sources that may assist an organization to select the controls needed for high value assets such as NIST SP 800-53 control catalog. More advanced controls and enhancements can be found in the CISA High Value Asset Overlay.

9. Conclusion

Cybersecurity is becoming more of an issue for states, communities and the private sector as the number and types of attacks that they experience are growing and becoming more sophisticated. Organizations need to have a comprehensive understanding of their critical assets, also called high value assets (HVAs), to enable them to prioritize and enhance their defenses against cyber-attacks. The federal government has issued many directives to assist federal agencies to identify their HVAs in order to understand potential impacts to those assets from cyber incidents and to enable them to ensure they are protected. Through these federal directives, a HVA Program has been developed for federal agencies focusing on national security. The national focus will not apply directly to SLTTs and small to mid-sized private organizations, therefore, a new model must be established and is described in this paper.

The first step in identifying HVAs is to analyze the organization's mission and to determine what services and functions are essential. A criterion is established and rationale to assist the organization to have a standardized method to identify the mission essential functions and critical assets that are essential for the operations of the organization as a whole. Once the MEFs and critical assets are identified, a method to prioritize them needs to be completed resulting in an inventory of the HVAs. This prioritized HVA inventory will show which HVAs if compromised would have the most damaging impact to the organization.

Most organizations do not have a formal HVA process. Formalizing the HVA model into the organizations governance structure will assist the organization to become better at maintaining proactive defenses, provide them with actionable information to make better decisions in regard to their most valuable assets, and better prepare the organization for the future.

10. References

[1] Center for Strategic and International Studies, "Significant Cyber Incidents", available from

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[2] Accenture Security, "2020 Threatscape Report", available from https://www.accenture.com/us-en/insights/security/cyber-threatscape-report
[3] CFI, "Asset Valuation", available from https://corporatefinanceinstitute.com/resources/knowledge/finance/asset-valuation/
[4] Flux Connectivity, "What is the Difference Between Standard Cost and Average Cost?", available from https://fluxconnectivity.com/what-is-the-difference-between-standard-cost-and-average-cost%EF%BB%BF/
[5] Office of Management and Budget, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government", available from https://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-16-04.pdf, October 30, 2015.
[6] Radack, S., 2004, Federal Information Processing Standard (FIPS) 199, Standards for Security, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], available from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150427
[7] Ward, M., & Subramanian, S., 2020 Deloitte-NASCIO Cybersecurity Study available from https://www.nascio.org/wp-content/uploads/2020/10/2020-Deloitte-NASCIO-Cybersecurity-Study-1.pdf
[8] MS-ISAC, 2019 Nationwide Cybersecurity Summary Report, available from https://www.cisecurity.org/ms-isac/services/ncsr/
[9] ICMA Cybersecurity 2016 Survey, available from https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf
[10] DHS, 2020 National Preparedness Report, December 22, 2020 available from https://www.fema.gov/sites/default/files/documents/fema_2020-national-preparedness-report.pdf
[11] Office of Management and Budget, "Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program" available from https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf, December 10, 2018
[12] DHS, List of Validated PMEFs by Department/Agency, 2015 available from https://www.dhs.gov/sites/default/files/publications/list_of_validated_pmefs_by_department_v2_fema.pdf
[13] Ruefle R., "Critical Asset Identification (Part 1 of 20: CERT Best Practices to Mitigate Insider Threats Series)", SEI Blog, available from https://insights.sei.cmu.edu/blog/critical-asset-identification-part-1-of-20-cert-best-practices-to-mitigate-insider-threats-series/, April 12, 2017
[14] Cybersecurity & Infrastructure Security Agency (CISA), Secure High Value Assets, available from https://www.cisa.gov/publication/secure-high-value-assets