Vormetric, Inc.

Response to

NIST - Developing a Framework To Improve Critical Infrastructure Cybersecurity

April 8, 2013

Submitted by:

Wayne Lewandowski
VP, US Government Sales
540-454-9075 cell
wlewandowski@vormetric.com

1. Overview

Vormetric is pleased to submit the following RFI response to NIST. We carefully reviewed what areas of the RFI we felt most qualified to answer. Although we did not respond to all questions, we do feel our comments were well thought out and meet specific needs that have been expressed in the document, as well as in the recent workshop on April 3, 2013.

As a data centric security company, we feel the cyber framework is a forward step to protecting data that meets the needs of the US government internally, our citizens, support contractors, and allied forces that we engage with to meet our interests.

As stated in a recent report by Mandiant, "100% of all data breaches involve stolen credentials". A recent Verizon Data Breach Investigation report in 2012, stated that "less than 1% of breaches occurred on end user devices compared to 94% on servers". The trends are there, data is being compromised at an alarming rate through compromised credentials, and our adversaries are focused on the high density targets of servers. This has an impactful result to citizen data (personally identifiable information – PII), government content, mission sensitive information, federal contractors, and items of national interest. The impact of data breaches can affect our way of life and security, continuity of government, and ability to secure information dominance in our efforts against terrorism.

Vormetric, brings a powerful platform to the market to assist in securing the new currency, data. Regardless of the data being structured in a database, or unstructured content (i.e. e-mail, sharepoint, images...), we provide a "data firewall" to separate data from the user. This capability allows separation of duties and reduces the attack space in the enterprise. Some key capabilities that can be enabled with the platform:

- Root/SysAdmin users have no access to data, just metadata and file structure so they can perform their jobs.
- Data access is controlled by applications, access, and actions. Confirming control of the who/what/where of data access.
- Robust reporting to ensure immediate information to what is occurring in the enterprise. This is easily implemented with applications that may already be in the environment.
- Remote crypto shredding of data and enterprise Keys to wipe access to forward deployed servers or compromised data centers
- Versatility to support Windows/LINUX/UNIX across NAS/SAN/DAS storage devices
- Support of Cloud, Big Data, and virtualization initiatives in the enterprise

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

   The greatest risk to improving cyber security is to the possibility of leaking confidential, secret, personal and financial data. Government as well as industry need to reduce the attack footprint and minimize any risk to data being compromised.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

   Uniformity in protecting data. Being able to determine a standards based approach(CC), and allows the largest freedom to choose infrastructure that is vendor agnostic

3. Describe your organization's policies and procedures governing risk generally and cyber security risk specifically. How does senior management communicate and oversee these policies and procedures?

   As an organization, we see our client's and partner's adopt multiple counter-measures to mitigate risk to data, infrastructure, and disruption to business/mission. Regarding data access, we see 5 layers or vectors of access to data that is deemed sensitive.

   - ***User/Presentation***
   - ***Application, Database***
   - ***System***
   - ***Storage***
   - ***Access controls around system and storage. Limiting access to the data by administrators.***

4. Where do organizations locate their Cyber Security risk management program/office?

   Frequently it is centralized within the enterprise, and it is often recommended that DR and failover sites are created to maintain availability of response to incidents.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

   A best practice of how to define and measure a risk by breaking into 3 pieces:
   - ***Personnel – How many individuals can influence this risk – positive or negative***
   - ***Probability – What is the probability of this risk being exploited***
   - ***Collateral Damage – What further exposure or damage can this risk introduce.***

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

   Cybersecurity risk management can range from a single individual maintaining all aspects of security to several segmented departments handling different aspects of risk to an organization.

   Information Security is a multi-front battle, and depending on the size of the organization, the extent of risk management varies. Larger organizations traditionally create specialized practices for each battle front – i.e. Network Security, Systems Security, Data Security, Endpoint Security.

   Organizations should look at cybersecurity as a multi-dimensional approach. Banks and the financial industry are well aware of this. There has to be an understanding of risk at a governance and compliance layer and there needs to be an understanding of technical risks as well as risks to the network layer, the operating system, and the application layer.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

   Most organizations, through regulation and risk mitigation are taking a data centric and system centric approach rather than focusing on the perimeter edge including endpoint access. By reducing the threat surface, they are able to repurpose their efforts and resources to combat real time events at the network edge by ensuring that the data has been protected and the risk has been mitigated at the system/storage/database/application layer.

Vormetric best practices support:

- ***separation of duties***
- ***key separation from the data***
- ***application independent security***
- ***integration to enterprise security architecture (SIEM, NGFW, reporting functions such as Splunk)***

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Organizations believe that security needs to be more efficient, transparent, strong, and easy to implement. Combining these four pillars and adding strong security protection schemes, organizations can begin to arrive at performance levels that are not impacted by cybersecurity controls.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Yes, Standards and organization bodies play a critical role in helping to define critical infrastructure cybersecurity standards, however, it must be framed by industry in collaboration with participating companies and nations.

As part of the Information Security standards, there is a distinct need for Data Security standards, that focus on the data itself, regardless of the infrastructure, architecture, or organization.

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

Data Centric security where you apply firewalling practices to the data itself(Criteria = Effect). Data should be only usable by appropriate users/processes/applications. The inherent concept of data being regulated or managed by privileged users introduces a security risk to the data just by being accessible to a user who may have no need to see the data.

2. Which of these approaches apply across sectors?

Today the approach of data security is the administrator or root account has all the authority to manage data on a system. This problem is not specific to any specific sector and needs to be applied uniformly across all sectors.

3. Which organizations use these approaches?

Using data centric controls is emerging as a standard across all types of orgainizations; from the Intelligence Community, financial institutions, healthcare, service providers, to media companies. The need to secure sensitive data is universal to all organizations.

4. What, if any, are the limitations of using such approaches?

Today the limitation is lack of understanding of the risks. Without understanding the risk of data leak and compromise a lack of action results in a vulnerable organization.

5. What, if any, modifications could make these approaches more useful?

The approach to data security needs to be a foundation of any implementation of every system. Security should be designed in from the start and monitored and managed centrally. Security controls also need to provide visibility and auditing.

6. How do these approaches take into account sector-specific needs?

A "data centric" approach to security can be implemented cross sector. By doing so, provides many sector-specific needs based on this approach.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

All sectors of industry can benefit from those with more stringent requirements. The framework being assembled through NIST (this very RFI) provides a much needed collaboration for all sectors to benefit.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

   Certain sectors, by their very nature of their business process, employ robust security technology and processes. Such as DoD and the Intelligence Community. Where possible, other industries should adopt those programs and policies that make sense for a given security standard or guideline.

9. What other outreach efforts would be helpful?

   IAC, AFCEA are examples of other entities that could be utilized as outreach efforts for industry and government sectors. Each of these have active cybersecurity working groups already collaborating on federal requirements.

Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;

  Key management should be centralized and kept separate from the data it is used to protect.

  The stringent use of "separation of duties" should be employed, keeping separate those that create keys, from those that create policies. Also, backup and audit functions should be kept separate. Critical processes such as backup recovery should employ "split key" technology.

- Identification and authorization of users accessing systems;

  Understanding what users are using your privileged accounts is critical. If a root account accesses data, who used the root account. Vormetric can track what accounts are used to access critical data but also keeps and reports on the chain of that login. If user "joe" logs into the system and uses su to get root

privileges then our auditing shows that "joe" accessed data with the root account. The root account can also be blocked from accessing critical data – even when root is the owner. We utilize encryption and the ability to decrypt sensitive data can be narrowed down to a minimal set of users and processes to minimize the attack surface on your critical data.

This approach is much more transparent to system administrators and doesn't require changes in their daily workflow unlike other systems that require close management of who can use privileged accounts.

- Asset identification and management;
- Monitoring and incident detection tools and capabilities;

Need to be employed as part of a layered security approach. All security systems should report their syslog (events) to a centralized collection and correlation system for analysis and reporting/alerting

- Incident handling policies and procedures;

Security products need to deliver both protection and information. Your data security products need to not only protect and control access to sensitive data but also provide information on what threats and access attempts are denied access to the data. This information should be able to be consumed by an overall event correlation product to feed the overall security picture of your network.

- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

By virtue of insulating the data from privileged users administrating systems you greatly reduce the risk of compromised credentials. Further, data that is summarized in big data or similar reporting tools can suppress PII, and other personally sensitive data. If needed, access can be granted on a case by case basis. An example would be a health research project that gathered stats on a patient group. If an anomaly was found that was unique or could be critical to that individuals health, a user of the data could be "read in" to access their specific personal info that was other was suppressed in the data output.

1. Are these practices widely used throughout critical infrastructure and industry?

Depending on the size of the organization at least, in part, most of these items are in use. The implementation varies. E.g., key management not being centralized, DR sites not fully replicated or tested on a frequent basis.

2. How do these practices relate to existing international standards and practices?

There is overlap and for the most part, congruent in functionality. However, some international (EU) practices are much more stringent. Based on nation laws and privacy concerns, there may be differences.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Security controls are moving closer to the data. This trend is growing in the industry and the understanding that you cannot catch all threats at the perimeter combined with insider threat many practices are locking down the sensitive data instead of relying on external controls.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

   These security practices should be utilized across all areas of business and mission. All industry will have some form of PII data, financial, medical or otherwise that must be secure.

5. Which of these practices pose the most significant implementation challenge?

   Vormetric believes that by adopting a data centric and system centric approach to security, industry can easily implement security controls and practices that are transparent, strong, and efficient.

6. How are standards or guidelines utilized by organizations in the implementation of these practices

   Guidelines and standards such as HIPAA and PCI, provide guidance into the technologies that need to be used to satisfy the Standard. Technology should not, however, be considered simply in order to "check a box" that a particular standard requirement is met. Functionality of the security solution must be tested against the four pillars of a successful security

implem*ent*ation: Easy to implement, provides strong encryption of data, transparent to the user community, efficient in so not to burden systems, processes with added overhead.

9.What risks to privacy and civil liberties do commenters perceive in the application of these practices?

By following standard and guidelines such as HIPAA/HITECH, PCI, SOX, Pii data should be protected as well as reduced impact to civil liberties. "They that can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety"

Exposure of PII, risk of identity theft. Crosses many areas/sectors. Banking, e-commerce, financial trading, healthcare, insurance, research, higher ed.

11.How should any risks to privacy and civil liberties be managed?

Ensure that PII data is suppressed from the content. Also, utilizing encryption with strict policy enforcement over user access to data. This should be surrounded by event logging and audit to centralized logging servers for alerting and reporting.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Adding to a layered security approach, SEIM correlation of event logs. In addition, addng database monitoring to all database implementions. 96% of all records breached are stolen from databases (souce: Verizon data breach report – 2012).