RFI RESPONSE

A Framework to Improve Critical Infrastructure Cybersecurity

National Institute of Standards and Technology, U.S. Department of Commerce

April 8, 2013

THE POWER TO KNOW®

Contact Info

Laurie Cook
Senior Account Executive
(571) 227-7000 x51777
Laurie.Cook@sas.com

Table of Contents

Introduction

Analytics and risk management perspective

SAS Institute has been the leading provider of analytic solutions for the past 37 years. As such, SAS' intent is to respond to the NIST Request for Information to provide guidance on developing a Cybersecurity Framework from an analytics and risk management perspective only. Throughout the response, SAS will articulate perspectives from its customers' point-of-view as well as where SAS sees the cyber market trending.

Common challenges

From SAS' customers' point-of-view, many enterprises follow a common paradigm. That is, most customers first establish Security Operation Center (SOC) for cybersecurity. This clearinghouse is the central focal point for defensive cyber activities, and typically responsible for maintaining situational awareness for the cybersecurity landscape within the organization. Co-locating resources and pooling analytical and investigative talent helps to ensure efficiency in handling complex threats such as cyber adversaries. However, organizations often overlook the need to implement a fully integrated analytical environment to identify overarching patterns and trends across the numerous layers of cybersecurity. Without an enterprise analytical framework approach in the cyber domain, it becomes very difficult to establish tactics, techniques, and procedures (TTP) of bad actors and behavioral signatures. Identifying these complex patterns of activity from the perimeter into and across the network provides valuable insight, which can then be analytically modeled and added to the defensive posturing at the perimeter level. This approach also assists in validating attribution which can be complicated through deceptive processes.

Best practices: a centralized risk repository and a hybrid approach to analytical risk management

From the market's point-of-view, SAS has seen many customers move towards an enterprise framework, where cyber is just one risk that needs to be managed. That is, one best practice in an enterprise cyber framework is the use of a centralized risk repository. Ongoing monitoring of network activity, both inside and on the perimeter, combined with applying advanced analytics provides the best tradecraft in assessing risk and alerting on critical events. A hybrid approach to analytical risk management has long been a best practice for enterprise fraud detection and can be leveraged within the cyber domain as well. The hybrid approach combines a rules-based method for known threats with advanced statistical analysis, such as anomaly detection, predictive modeling, and network analysis. This highly effective approach identifies behavioral attributes that are indicative of cyberattacks, reduces false-positives in the alerting, and results in detection of threats as early as possible to mitigate the threat or reduce the loss of critical assets.

A 360^{o} view of the network for enterprise risk management and analytics for foresight

This environment offers a range of techniques and processes for the collection, classification, analysis and interpretation of data to reveal patterns, anomalies, key variables, and relationships that would otherwise be obscured or invisible. The goal is to have a 360 degree view of the network at all times to better manage risk from an enterprise level. To establish a truly comprehensive Cybersecurity Framework, it is necessary to incorporate advanced analytics into the model to see what has happened in the past, what is happening today (real-time), and to see what could happen in the future. By adding advanced analytics to the nine core practices of a critical infrastructure, cyber defenders can stay one step ahead of would-be hackers while protecting the most critical and sensitive information within the business.

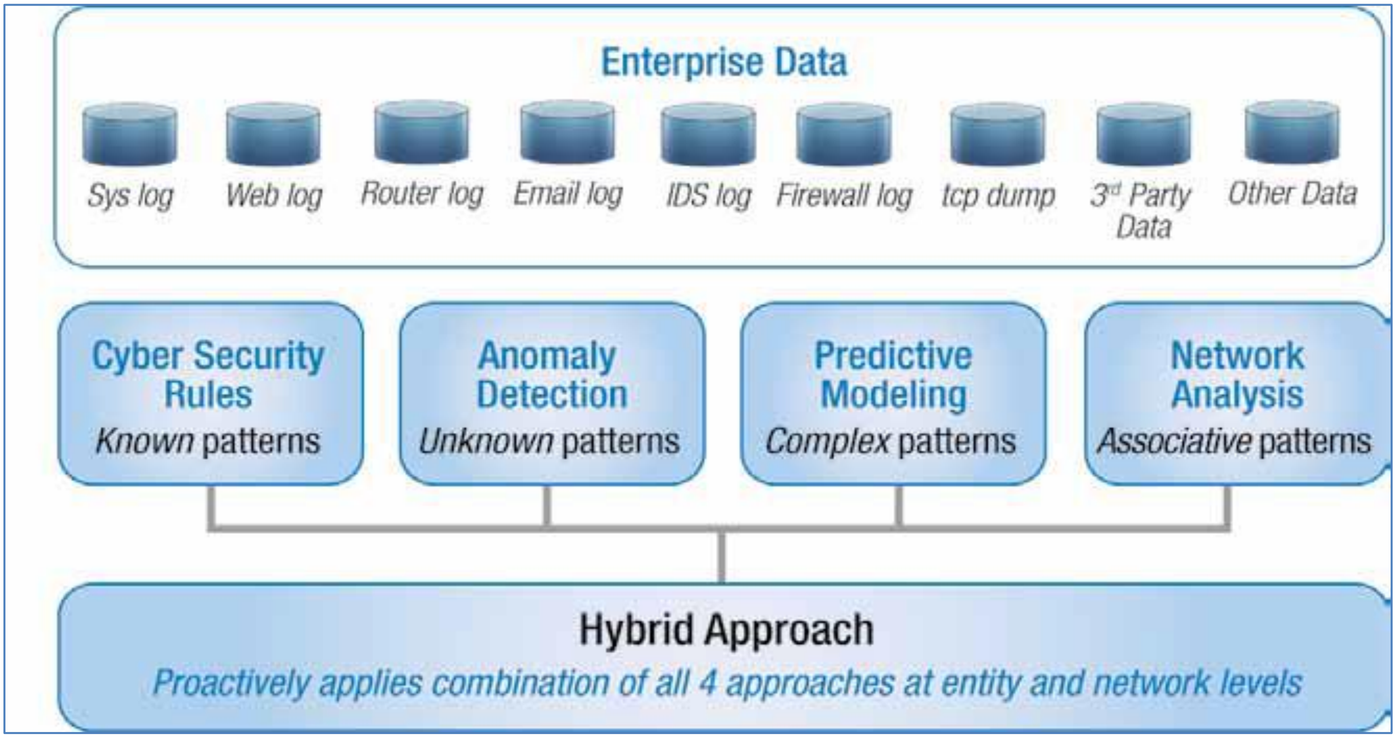

Figure 1: A hybrid approach to analytical risk management.

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

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

Challenges: tight budgets, governing internet access and protecting personal information

The goal for all organizations, including government, is to have a greater reach and presence with employees as well as customers, and to provide these services in a secure manner. Common challenges include:

- Budget remains a great task for improving cybersecurity. It is only after an organization experiences a cyberattack that budget becomes readily available to address future assaults.
- Governing user (employee) access to the internet is one of the greatest challenges around improving cybersecurity practices. Granting internet access to employees without any restriction to what they can view or download creates a vector for access to the network, including what can be done unintentionally or deliberately.
- Assigning proper classifications and importance to various data sources allow for data to be protected at an appropriate level based on the sensitivity. While secure organizations understand and handle data classification appropriately, this is not commonplace outside of this specific user population.

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

Prioritizing the criticality of internal information

The greatest challenge to creating a cross-sector standards-based Framework for critical infrastructure is prioritizing the criticality of internal information based on the risks that these challenges face. For example, within SAS Institute, there are three business entities: SAS Institute Inc, SAS Solutions OnDemand, and SAS Federal LLC. Since each group addresses vastly different markets, the goal of creating a standards-based Framework becomes a challenge.

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

Risk policies and procedures

This commenter's organization leverages our risk-based pedigree to apply risk metrics and ratings to various operations and behaviors. We have found that this approach allows for the organization to better address and assess the current status of its systems and services. To ensure this risk approach is appropriately enforced, it is governed using the approaches and controls outlined in the organization's Risk Management Policy. This policy cannot be disclosed, as it is deemed sensitive to the organization; however, standards for information security should include risk factors and mechanisms, which should be enforced by the Chief Information Security Officer's office.

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

Chief Information Officer typically oversees information security

Most information security systems and programs operate from within or are aligned with the Chief Information Officer's role in the organization. This alignment offers both additional capabilities, and likewise, introduces challenges. The separation of duties associated with distinct, separate reporting chains allows for better isolation and an oversight layer for information technology. The integration of the information security and information technology functions provides a more cohesive approach for a budget conscious organization to approach cybersecurity, as better security practices and procedures can be injected into standard processes; however, this may occur at the cost of oversight.

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

General risk management process

Generally, risk management is a process whereby the risk of an event occurring is balanced against the actual likelihood, impact, and mitigation associated with an event; offering an overall risk. Most organizations apply some level of risk management to most processes, including things such as where to build a new building or warehouse. If an organization should increase its presence into a new market,(or any other example where external factors need to be weighed and balanced in terms of risk versus reward to an organization), this becomes a risk tolerance exercise for the organization.

Risk portfolio components

Organizations leverage components of the risk portfolio, such as intellectual property, copyrighted material, patents, and trade secrets. Each of these factors are all integral parts of protecting assets and potentially lowering risk through legal and process mitigation strategies.

Risk mitigation for cybersecurity

Cybersecurity-based risk, however, is a combination of potential events and activities, as well as the potential threat vectors that exist within an organization. Methods and techniques utilizing standards and strict process adherence can assist in lowering the risk or partially mitigating risks associated with cyber events. However, they cannot eliminate the risk, as the threat vector associated with risk is too broad to be eliminated, even with a comprehensive risk mitigation plan leveraging only process and standards.

Comprehensive cybersecurity risk strategy

For a cybersecurity risk strategy to be more comprehensive, it should incorporate not only process and standard-based mitigation, but should include threat profiling and behavioral analysis to account for unforeseen and potentially unknown areas of cybersecurity risk. Additionally this strategy should incorporate and fuse internal device data, as well as external threat data feeds, which provide behavioral analysis associated with new events and techniques used to defeat network and device protection capabilities.

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

Today's computing environment increases cybersecurity risks

As organizations leverage a more open model, whereby solutions such as cloud computing are heavily leveraged, and employees are allowed to bring personal mobile-based devices to work, the risk associated with a more global presence is more evident than ever before. In traditional network and information security, a perimeter could be set and guarded vigorously. While the perimeter is still present, the devices, which actively move from behind the perimeter to outside of a company's network are ever increasing. This dynamic, flexible computing environment is providing organizations with economies of scale, but in many instances, at the cost of information security.

Cybersecurity risk management is critical to enterprise risk management

One of the only avenues to combat this dynamic unknown is to assess the risk of what is known and understood about a specific connection, device, or entity. Once this information has been gleaned, data enrichment should be performed with behaviors that are considered to be normal and abnormal in the communication flow of a node on a network, or a network connection to an organization's infrastructure. Cybersecurity risk management is a key centerpiece in the arsenal of an organization's information security strategy, as it assists with the prioritization of events and makes the mitigation of these events known.

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

SIEM tools provide real-time analysis of security alerts generated by network hardware and applications

Organizations are leveraging a combination of tools, techniques, and processes to address the challenges of cybersecurity. The tools commonly used include Security Information and Event Management (SIEM) offerings, such as HP ArcSight and Q1 Labs, which provide a basic level of insight into events that are happening on the network. Additionally, products such as firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) are commonly in use within larger organizations. These devices can capture information which may characterize network traffic flows, but do not provide real insight into what the data means, nor do they review data over a long period to detect trends and abnormal behaviors.

Risk management techniques and processes

Common techniques and processes include:

- Manually correlating events on the perimeter and events occurring on the network nodes,
- Reviewing web information concerning new and emerging attacks found on networks,
- Enforcing proper security configuration on devices, whereby open communication ports are available, if necessary, for business purpose,
- Prohibiting communication avenues not required for business success

Standards provide additional guidance

Combining these tools, techniques, and processes with standards, such as the concepts of least privilege and others listed in the NIST 800-53 security controls, are commonly used to act as guidance to security or technology personnel. Other guidance such as the Trusted Computing Platform from Microsoft, and NSA guides on secure computing provide an organization level framework. This assumes that the organization understands the value of information security and is committed to the safe computing process and enforcing these practices on employees and others utilizing network or organization resources.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

HIPAA regulatory requirements

The only regulatory requirement enforced on our business is HIPAA, relating to the use and practices surrounding Health and Human Services data. While this regulation applies to most organizations, it is understood that many establishments in other critical areas of infrastructure are governed by various regulations or standards which would recommend the reporting of cyber events to the appropriate state and/or federal entity for, a minimum, information sharing with other entities.

Information sharing

Programs which promote information sharing between government and industry, such as the FBI's InfraGuard program should be highly leveraged in any new standards and potential reporting requirements that are recommended under this Cybersecurity Framework.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water and transportation sectors?

Interdependent critical infrastructures

Oftentimes, organizations leverage the standard mechanisms such as power, cooling, and technology redundancies. These redundancies may not be individualized to an organization's industry, but could and should be adopted nationwide.

Power redundancies

The power redundancies include multiple power feeds from separate entry points, battery backups, and potential use of generators for long term power sustainment. This, as most, requires the use of the electrical grid and power generation sectors as a requirement on the critical infrastructure.

Cooling redundancies

Redundancy for cooling and other environmental capabilities come to the majority of organizations through the use of backup environmental controls and cooling units. The cooling facilities in most organizations include water based devices, thereby incorporating a reliance on the water treatment critical infrastructure.

Technology redundancy

Tools utilized for technology redundancy include redundant network routes and devices (e.g., routers, switches, load balancers, etc.), self-healing internet connections through different providers, leveraging different media types and different points of presence, redundant array of inexpensive disks (RAID) configurations, and redundancy in shared devices and storage. These technology redundancies all rely on the power infrastructure, as well as manufacturing and transportation sectors to ensure the original and support parts are able to be delivered.

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

SLAs to meet performance goals

Most organizations have adopted service level agreements (SLAs) to provide guidance and expectations as to availability of critical services. However, most do not provide governance concerning availability of services as a result of cybersecurity risk. No metric other than SLAs are currently in use to govern availability due to cybersecurity events.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

Reporting requirements

As a service provider to the Department of Health and Human Services, the organization is required to comply with HIPAA regulations.   At this time, there has been no request to provide DHHS with any structured reporting.

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

Very few countries have online and electronic laws

Governmental standards, and in some cases, tools or capabilities, such as the Trusted Computing Platform guidance from Microsoft and NSA guides or secure system configuration would be an important step in creating a cybersecurity conformity assessment. While these recommendations are on a national level, it is important to note that these fundamentals could be adopted internationally as well. However, prior to international standards being implemented, it would be necessary for additional countries to implement and enforce online and electronic law. Otherwise, these standards do not lend themselves for easy adoption.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions. NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations. NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

Limitations of existing policies and standards

Many organizations are challenged in the area of cybersecurity as none of the existing policies or standards are comprehensive in nature, and do not provide an exact blueprint for an organization to achieve a secure cyber posture. Some cyber-professionals assert that a combination approach of various standards and policies, which may potentially complement each other, could provide the most comprehensive approach to the policy aspect of cybersecurity related issues. Many organizations have begun adopting some combination of policies, as these are used in numerous aspects of continuity plans and disaster recovery plans, and may be required in certain lines of business.

Leveraging fraud detection best practices from the financial services industry

Most businesses take precautions to protect infrastructure and data by way of traditional approaches, which include deploying firewalls and other network intrusion tools for tactical cybersecurity. However, without best practices guidance available, it may be beneficial to examine how the financial services industry approaches fraud detection as a potential strategic approach to cyber-defense. This study could provide a valuable in-depth understanding of adversarial motives and tactics, which can enable an organization to better defend against cyberattacks.

FFIEC risk management framework

One example of the synergies between financial services and the information security sectors occurred in June 2011 when the Federal Financial Institutions Examination Council (FFIEC) formally released the long-awaited supplement to its “Authentication in an Internet Banking Environment” guidance, first issued in October

Risk management controls to authenticate the identity of retail and commercial customers accessing internet-based financial services

2005. The supplement reinforces the risk management framework described in the original documentation and updates the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment. This holistic risk approach guided the official supplement and highlighted the need for:

- Better risk assessments
- Effective strategies for mitigating known online risks
- Improved customer and employee fraud awareness

Layered security approach

Many of our top financial services customers have collaborated with our organization to understand how technology would be able to play a key role in support of this new supplement. For example, layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. We work with our clients in supporting this layered approach specifically in fraud detection and monitoring systems. These methods include consideration of consumer history and behavior through a unique customer signature approach as well as a timely, informed and effective institution response decision on 100 percent of an organization's customer transactions in real time.

Other sources of industry best practices that our organization monitors include:

- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- BITS, the technology policy division of the Financial Services Roundtable

A piecemeal approach does not provide a global view

Many organizations begin by using existing cyber tools stitched together to address various cyber issues. These solution components leverage standard SIEM tools, firewalls, perimeter security solutions, etc., but do not address the goal of providing a global picture of the systemic health of networks, applications and so forth. To get a global view, data from these systems must first be fused together into a cohesive structure that represents all entities within the operational environment.

Limitations of using forensic analysis alone

Once in a common structure, many customers use visualization techniques to do a forensic analysis in order to determine vulnerabilities, visualize attacks, identify affected systems and services and evaluate operational readiness. While forensic analysis will help identify long-term vulnerabilities and provide case evidence to law enforcement, it does little to protect against 0-day threats and does not provide a set of countermeasures that can be employed in real time.

The need to detect attackers in real time

To deal with these threat vectors, any cybersecurity solution must provide a capability to handle massive amounts of data, while providing security analysts a visual representation of events either as they transpire, or in a forensic manner after the fact.

2. Which of these approaches apply across sectors?

Risk techniques have horizontal applicability

Organizations should apply risk techniques that are horizontal in their application to the enterprise. These systems should view the cyber problems in the context of overall enterprise risk management solutions, such as those used in the financial sector. An example of this is risk scoring which has been proven as a best practice in mortgage lending, credit scoring, insurance, and securities, and is equally applicable to cybersecurity.

Analytics and advanced big data techniques

Notwithstanding, cyberattacks are alike in nature to traditional financial services fraud. A big data/volume of "transactions" through credit cards swipes is similar to cyber access attempts with results (i.e., approve/deny or access/denial of access) both happening in rapid succession. Seeds of a paradigm shift can be found in credit card fraud detection, which offers a comparable use case for cyber threat detection. For fraud detection, banking organizations needed to gather the skills to detect fraudulent behaviors, primarily through an increase in the number of channels used to communicate with customers.

Circumventing the system

In the cyber world, an intruder will test his/her permissions and any alerting that has been put into place on the now compromised host, by making changes to unimportant files, and adding new files to a deeply nested directory. This test, while minimal, is the exact same principle as the small gas station transaction. This purposeful, and extremely important test, indicates that an attempt to compromise a system has ended in success.

With holistic access to an organization's data and enterprise analytics, organizations have the capability to identify and expose patterns and behaviors which are connected to risks, and can act immediately to reduce or eliminate threats. By embracing analytics with advanced big data techniques, organizations can control and automate the processes associated with assessing risk. This comprehensive approach enhances the cyber detection process, making it more accurate and sustainable in terms of detection and ultimate results.

3. Which organizations use these approaches?

Organizations tend to adopt these approaches only after significant losses

Unfortunately, organizations do not typically take precautions which can seem "costly" due to the resources or technology required until after a significant loss occurs. With fraud, the loss equates to monetary amounts which can be recovered. The cost to address this loss is offset significantly by the recovery or savings of funds, which often drives the decision to implement. For example:

- CNA insurance companies use predictive analytics to enhance fraud prevention

- HSBC Holdings plc, one of the world's largest banking and financial services organizations, uses advanced analytics to monitor and risk score the millions of transactions processed each day
- Los Angeles (LA) County uses social network analysis to uncover fraud rings relative to its child care services

In cyber, we are beginning to see a shift in this thought process. Given the expectation that everyone is susceptible to cyberattacks and the negative connotation associated with data breaches or information theft, along with the cost of recovery, the proactive approach is gaining momentum.

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

Limitations of visualization tools alone

The standard approach in today's operational environment is to empower cybersecurity divisions with a variety of visualization tools that allow cyber analysts and operators to monitor and react to cyber threats. Cyber professionals are growing more rapidly than other IT roles due to increased threats and the belief that a greater volume of individuals focused on the problem is the solution to preventing further incidents. Unfortunately, this approach is not only costly, but prone to error as sensor data volumes increase, and cloud architecture becomes more pervasive.

A multi-layered analytical approach

By taking a layered approach to prevention and detection through multiple analytical techniques, the risk of attack is lowered. However, some of these individual techniques can pose challenges and limitations.

Advantages of rules-based systems

For example, business rules have a distinct advantage in that they are both flexible and easy to understand. Most rules-based systems can be updated quickly with new rule logic without significant intervention. From a regulatory perspective, rules-based systems are typically preferred, as they can be easily explained.

Shortcomings of rules-based systems alone

The challenge, however, with rules-based approaches is that they encode only a small amount of information. Furthermore, rules-based approaches don't generalize well on new and unseen data because they are "information limited." The example above accounts for a situation in which a customer attempts to deposit a cash amount greater than $10,000. However, consider a situation in which a customer attempts numerous smaller transactions within a single day that together total more than $10,000 or a customer who purposely operates just below the $10,000 threshold. To address these patterns, the user needs to add more rules to the detection system. This trend will continue as the organization attempts to prevent the various new types of fraudulent activity. The result or byproduct is a growth in business rules that can create management issues, overlapping business rules, and a detection engine that is always a step behind. Despite their deficiencies, business rules have their place in fraud detection systems, as they provide a flexible, explainable method for detecting known fraud patterns. They can also be used in conjunction with other analytical detection methods. This is beneficial since business rules can be adjusted quickly, while analytical techniques typically take more time to retrain or build.

Gaming the rules-based system

Most existing information security solutions attempt to use static rules to define what is allowed or disallowed from areas or hosts on a network. This understanding has led to individuals or groups which want to exploit these security systems to understand how and what these systems weigh in their assessment, which has caused a game of cat and mouse to ensue. This game consists of a rules or signature provider to add content concerning behavior to disallow, and the perpetrator then attempts to slightly change their approach to an attack, to see where the lines are, thereby allowing for the system to be 'gamed', by taking advantage of what is allowed, disallowed, and the logic which is used to delineate between the two statuses.

Recommended hybrid approach

A hybrid approach to this problem will incorporate the use of existing rules or signatures, and will combine this static data with dynamic, intelligent analytic models, which will enable probabilistic events to be determined, potential outcomes to be weighed, and ultimately, nefarious behavior disallowed on public and private networks.

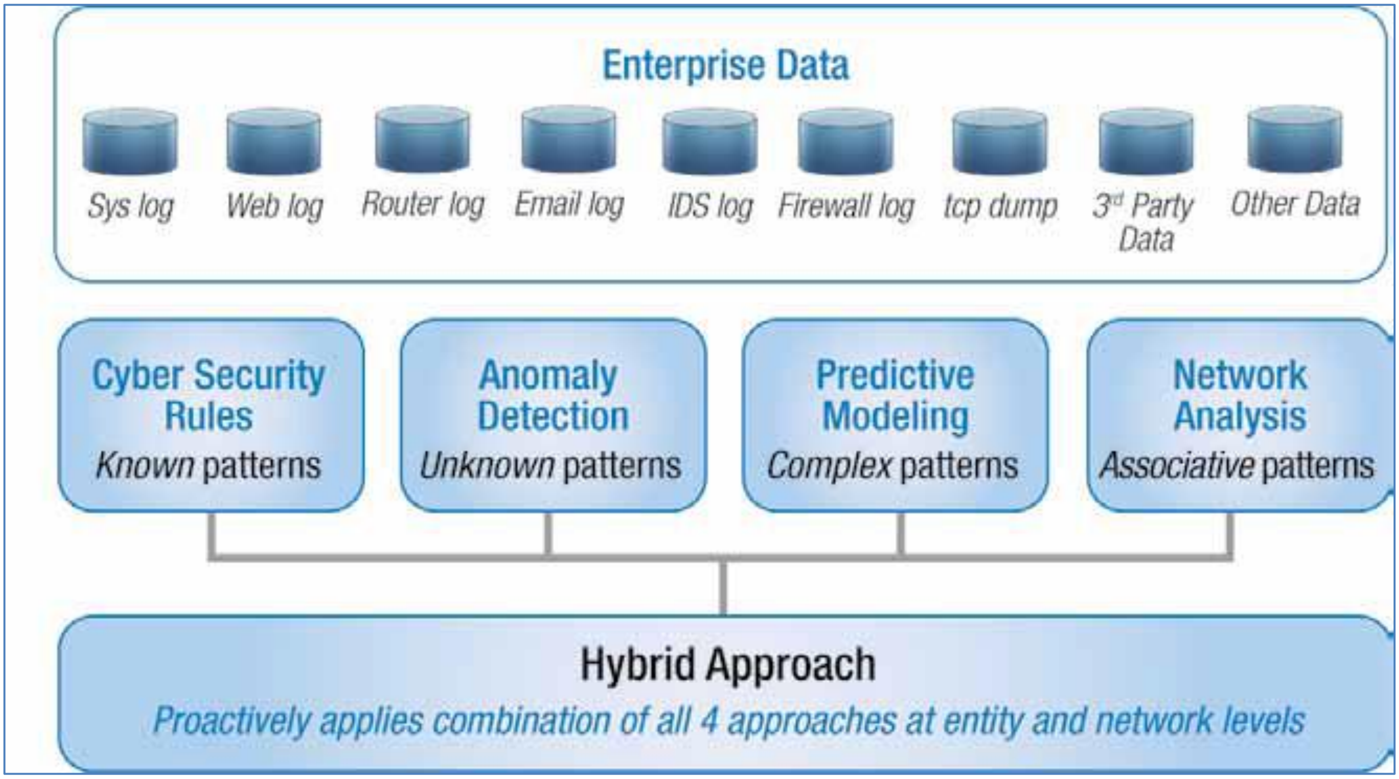

Figure 2: A hybrid approach to analytical risk management.

Anomaly and peer grouping methods

Anomaly and peer grouping methods were developed to address the generalization problems of rules-based detection schemes. Peer group methods attempt to compare the behavior of individuals or entities with their peer group. A peer group is a collection of individuals or entities with shared attributes—behavioral, demographic, or a combination of the two. Typically, business rules combined with clustering techniques (e.g., k-means) are used to segment populations and assign individuals and entities to specific peer groups. The behavior of an individual or entity is then compared to the peer group. Anomalies are found when an entity's or individual's behavior deviates from the "normal" behavior of the peer group. This method is popular with compliance applications, such as anti-money laundering solutions.

Limitations of anomaly and peer grouping alone

The challenge with peer grouping is, like rules-based approaches, its inability to generalize on new and unseen data. Another common challenge is that the behavior you are looking out for is often found to be the "normal" behavior of the peer group. And finally, there is the challenge associated with managing these types of detection systems. Typical implementations use large amounts of data to create profiles within databases. This process is time-consuming, thus adaptability comes at a significant cost.

Automated methodology/tools-based approach

The cybersecurity field is investing in additional headcount because they must rely on human interpretation and adaptability to new threat situation. However, given the complexity and significant volumes of data, an automated methodology/tools-based approach ensures balance between securing the network and allowing for ongoing mission needs.

Holistic or all-source risk assessment

Due to the complexity and numerous cybersecurity tools in the marketplace (network, application, data, insider, etc.), true cyber situational awareness can only be achieved through holistic or all-source risk assessment. By leveraging advanced analytics to correlate events and identify overarching trends and patterns through a hybrid analytical approach, organizations can determine overall risk across the enterprise. While these techniques are not new, the combination of hybrid analytics and recent advances in in-memory technology are enabling risk detection based on complex analytic models against big data.

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

Advanced analytics for near real-time threat analysis

The explosion of cyberthreats and sensor data has made cybersecurity a big data problem. Through advanced analytics, cybersecurity solutions can address the shortcomings of current security vendors by establishing normal behaviors and detecting variance from these norms in order to provide near real-time threat analysis for an organization. In other words, the cyber problem is really one of modeling a variety of situations such as adversary behavior, nominal behavior for internal users, cyber asset inventory, etc. and presenting results to a semantically rich visualization environment for cyber warriors who must make quick decisions to prevent data loss. For real-time operations, analytics can improve situational awareness by providing earlier detection of emerging threats resulting in earlier threat mitigation.

Automated process

The best approach for a challenge of this magnitude is to employ an automated process providing analysts with as much time-to-decision as possible. Considering cyber events can occur within nanoseconds, developing automated solutions are the only way to ensure detection or gain advantage against an adversary. Many of the cyber tools available today (e.g., firewall or SIEM software) automate many decisions to keep up with the ongoing number of the attacks. However, in the investigative and advanced analytics stage of bringing together all of the cyber landscape information and correlating events to understand the overall tactics, techniques, and procedures (TTP), the majority of approaches are still manual, depending on human intervention which is complicated by levels of expertise and training.

Next generation of threat detection

New ideas, methods, and technologies will dramatically improve cybersecurity detection efforts. This next generation of threat detection will use vast quantities of disparate data, distributed computing, rapid development technologies, and advances in predictive modeling to produce faster, more-accurate solutions to detection problems. The following are a few guiding principles behind these next-generation methods:

Use as much data as possible from a variety of sources

- Most detection systems rely on structured data in the form of transactions. It is a well-known fact that augmenting detection schemes with a wide a variety of data—including unstructured and semi-structured data—greatly improves the accuracy and generalizability of predictive models.

Engineer mass quantities of diverse features from multiple sources

- Predictive performance depends on how you manipulate data and create features (variables). Next-generation systems will make it easy to assemble, manufacture and test features with more diversity and more predictive power.

Analyze data "in steam" whenever possible to reduce detection and reaction time.

- Use of event stream processing technology (also known as complex event processing engine or CEP) can detect anomalous patterns in high volume, low latency streams of data. These suspicious patterns can then be further analyzed by more complex analytical models with the "scores" or results (i.e., an actual positive versus a false positive) and the results can then be sent back directly to the event stream processing engine to halt or re-route "bad" transactions" for further, detailed analysis.

Explore and visualize

- Creating and selecting the features needed to detect a pattern is 80 percent of the battle. While creating simple features to perform sums, averages, and counts over specific time ranges is relatively straightforward, it is much more difficult to engineer, craft, and test a feature that maximizes predictive power. Success lies in the ability to create, explore, and test potential features interactively on large quantities of data.

Keep it simple

- If you can detect something with a simple rule, don’t complicate things with models and peer groups. The minimum description length (MDL) principle says, “The solution that makes the fewest assumptions should be selected.” In next-generation of detection, complex analytics will be used to engineer features and rules for detecting events of interest.

Take a white-box approach to the black box

- A key limitation of current systems is the inability to provide insight into why something has been detected or how the current systems work. As the complexity of a system increases, our ability to understand the system decreases. Ultimately, what is needed from the detection engine is the story behind why something was detected.

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

Using data model and analytical techniques to address sector-specific needs

Sector specific needs are accommodated through the data model and analytical techniques that are applied based on the specific cyber threat they are facing.

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

Balancing cyber risk with organizational risk

Organizations should adopt an enterprise risk management approach to all aspects of an organization’s operation. Here, stakeholders would use an enterprise risk framework to balance organizational risk relative to each other depending on the context of the business. For example, FEMA must balance cyber risk versus the risk of hurricanes hitting CONUS. This overall risk assessment can be delivered to policy makers so that trade-off decisions can be made based on relative risks. At this level, true situational awareness and decision support systems deliver the same results.

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

Common practices can be leveraged across industries

Certainly, industry specific methodologies shared with the broader community can help larger cybersecurity goals. Financial Institutions face challenges involving access to monetary goods versus software companies which institute safeguards against their code, and leveraging common practices across industries or sectors can definitely help align efforts.

Information sharing

We would highly recommend that organizations such as US-Cert, the Carnegie-Mellon Cyber organization and the FBI’s InfraGuard groups all be heavily weighted in terms of organizations that have been created or have been given a mission to increase the data flow among various industries and government.

9. What other outreach efforts would be helpful?

Develop standards for data models and advanced analytic techniques

NIST should continue to develop standards that focus not only on policy, but also data models, risk modeling, and advanced analytic techniques. By clearly communicating these standards to industry, NIST could play the role of market maker, using its standards on information sharing, etc. to make it worthwhile for vendors to enter the market with their unique capabilities.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. 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;***
- ***Identification and authorization of users accessing systems;***
- ***Asset identification and management;***
- ***Monitoring and incident detection tools and capabilities;***
- ***Incident handling policies and procedures;***
- ***Mission/system resiliency practices;***
- ***Security engineering practices;***
- ***Privacy and civil liberties protection.***

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

Best practices found in the financial services industry

There is not a standard throughout all providers of critical infrastructure. In some cases, there are extreme inconsistencies across industries and verticals associated with critical infrastructure. A standard set of procedures modeled after practices in specific sectors would be most applicable and appropriate in this standard framework. The financial services industry reviews almost any event from the perspective of risk, which provides a truly unique view when looking at cyber occurrences through a risk assessment lens. Applying a risk framework to cyber allows for factors such as impact, likelihood, and mitigation strategies to become an important part of the calculation associated with newly established connections and their behavior. This same approach is exceptionally effective in identifying behaviors, such as attempted fraud, passenger screening, and intelligence-led policing within our country.

Establishing a true situational awareness capability within an organization

To accurately depict a user and his/her behaviors, a separation of business and operational systems should be implemented. Granting user permissions to change configurations in one area of the organization and not others will minimize the damage or risk to which a single employee can expose the organization. However, data concerning usage patterns should be consolidated into a single view, as these are patterns associated with a single individual’s behaviors. Practices such as data encryption, data security zoning, redundancy and resiliency systems, and others should be a recommended aspect of any security framework, and in conjunction, should produce logs and data which would feed behavioral analysis systems to achieve security intelligence. This intelligence information should be fused with outside sources, such as threat intelligence feeds from leading vendors and governing agencies, security posture assessments, antivirus and anti-malware systems and services, data loss systems, external source identification services, social media feeds, and perimeter device logging feeds to establish a true situational awareness capability within an organization.

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

International security concepts, methodologies, and practices are recommended by a risk management framework approach

These practices will further standards globally, as the international community is battling the challenges of a global cyber landscape, and has not established a set of guidelines that provide additional layers of security or auditing capability. The global community is ailing from the same vulnerabilities and attack vectors as areas within the United States. Certain international security concepts, methodologies, and practices such as the layering of security devices, perimeter security device inclusion, data segmentation, and classification are completely recommended by a risk management framework approach. Each model provides valuable input into the risk model and eventually, the risk rating associated with network connections and events. Practices such as encryption of data at rest, strong encryption for data in transit, session encryption for applications, and other best engineering, development, and architectural practices are recommended for any security intelligence framework for cyber applicability.

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

Priority order of core practices

The secure operation of critical infrastructure should follow the proper priority order for the practices put forth from NIST:

1. Monitoring and incident detection tools and capabilities
2. Security engineering practices
3. Use of encryption and key management
4. Incident handling policies and procedures
5. Mission/systems resiliency practices
6. Identification and authorization of users accessing systems
7. Asset identification and management
8. Separation of business from operational systems
9. Privacy and civil liberties

Complex behavioral analysis

The recommended priorities listed above incorporate a combination of reactive and defensive approaches that are necessary. Every organization must consider the amount of intrusion that has occurred previously, coupled with a proactive posture that thwarts attempted attacks prior to information exfiltration or resource hijacking.

A truly comprehensive fusion of multiple data feeds, event correlation on that data, and analytics are needed to provide complex behavioral analysis on network traffic.

Monitoring and incident detection tools and capabilities

The priority focus of these nine practices is monitoring and incident detection tools and capabilities. The logic behind this recommendation is that the mindset of most individuals is that systems and services inside the infrastructures have been compromised at some level, meaning an organization would be in a defensive, reactive position to keep sensitive information from leaving through the perimeter gateways. Monitoring would allow the organization to understand connections, both inbound and outbound from the perimeter, thus allowing abnormalities in traffic flow to be analytically established and shunned, if appropriate. This would also allow for the identification of nodes within the network that have been compromised through infections with malware, an insider threat, or remote access tools. A fusion of data sources is necessary to incorporate the feeds, internal log information, perimeter device logs, and existing risk information to make this information analytically operational.

Proactive approach

While monitoring and incident detection tools and capabilities are being matured in the environment as a part of the framework's focus, individuals working in the engineering, development, and architecture areas within an organization should be made aware of secure computing concepts, methods, and principles. This proactive approach allows for newly deployed systems and services to be implemented in a secure manner, utilizing the security standards derived in a Security Intelligence Framework. This process employs existing threat intelligence information, and fuses this information with the risk management framework to bring together a cohesive view of the organization's risk and security posture which is actionable.

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

Privacy and civil liberties protection is only necessary for PII info

Privacy and civil liberties protection is not as applicable for organizations or individuals, who have a web presence, but lack personally identifiable information (PII) or other "valuable" information (e.g., intellectual property, etc.). These organizations would not have the same cybersecurity needs due to the lack of "valuable" information to be illegally accessed. Consider, for example a historical society which does not operate an ecommerce website or another informational outlet.

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

Monitoring and incident detection tools and/or capabilities pose the most significant implementation challenge because these capabilities are currently not at a maturity

A single, unified cyber view of current situational awareness is needed

level to provide an organization with a single truth when facing cyber issues. The difficulty is partially caused by the cyber landscape and fragmentation associated with vendor approaches. The Cybersecurity Framework should call for a single, unified cyber view of current situational awareness. This single view would provide:

- A fusion of existing threat intelligence sources
- Open source data feeds (including social media) internal threat modeling and risk information the organization may already have)
- Perimeter security device logs, workstation and server logs, antivirus, and anti-malware software defense logs
- Any other source to provide a common single pane of glass into the current cyber posture of an organization

Reasons for inadequate situational awareness

This single view of situational awareness will provide Security Operation Center staff with a true depiction of existing status, which currently does not exist. There are many reasons for its lack of existence, not the least of which is the difficulty to fuse massive volumes of data to provide a single data set capable of providing the information necessary. Another reason which lends itself to the lack of situational awareness includes the vendor landscape, which promotes a single company or product capability to provide whatever is necessary. This is simply not possible given the massive gaps in current product capabilities. No single device, appliance, software package, or piece of hardware can provide the combined capability required.

Big data is another challenge

The framework should promote a holistic view and approach to cybersecurity. Undeniably, many aspects of cyber make it incredibly difficult to detect and properly defend. Some information factors currently include the sheer volume of the data that is generated, as well as finding and retaining the data of value. The challenge becomes not discarding the data which may not show the same level of value. This is due largely to, the speed at which data is generated forcing most organizations to retain only subsets of information, as otherwise additional hardware costs must be incurred. The framework should include a section specific to the handling of “big data”-like volumes of data flow, as this is a major stumbling block to most organizations’ approach to monitoring and incident detection.

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

Adoption of standards varies by industry and risk tolerance

The utilization of standards and guidelines are partially dependent on the industry and/or vertical within which the organization operates because the requirements, mandates, operating behaviors, and norms are varied depending on these factors. Some organizations will actively review and adopt practices that allow for a decrease in the amount of risk exposure within a business practice. It is likely that organizations will implement guidelines which are relatively inexpensive to implement based on hardware, software, or services and associated labor. This occurs partially because organizations will weigh the cost versus the perceived value of the protection that is provided as a result of the security practice implementation. The risk tolerance of the business will directly align with that organization's experience with cyber events. Cyber budget restrictions tend to loosen only after a threat has occurred.

Budgetary constraints hinder standard adoption

As the Cybersecurity Framework is specifically addressing the critical infrastructure within our country, the regulatory requirements on operators will often vary in terms of inspections and verification of services and capabilities stated by operators. However, a hindrance to widespread adoption is the cost associated with an implementation or service which exceeds budgets or was not properly anticipated. Consequently, a recommendation or best practice may become delayed or even cancelled due to budgetary constraints. The issue remains that while the framework allows for operators to balance the cost associated with a mitigation versus the likelihood and impact associated with an event, the ultimate victim of a cyber-event will not be the business, but instead the organization's consumers of services or products. The critical infrastructure sectors are likely to be hesitant to accept the necessary nature of the costs associated with services and systems which provide best practice or increased guidance due to the budgetary climate in both business and government.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Lack of process and funding for IT standards

Currently, many organizations do not look to themselves for IT standards, and simply adopt practices that already exist in the marketplace. This causes a fracture of sorts, in that most organizations supply IT services as a method of meeting the organization's goal, which is not normally to supply IT services, but instead, to provide services or products within the industry they operate. This creates a segmentation of IT spending from the rest of the direct revenue generation portions of the organization. A lack of proper funding generally accompanies this segmentation.

IT systems viewed as business enablement rather than security mechanisms

Largely, organizations attempt to use best practices in IT standards for the purpose of automation and not for the purpose of security per se, since the directed purpose is to maintain systems and services necessary to enable revenue generation portions of the organization without interruption. Organizations, such as Marriott, Best Buy, and Whole Foods are not in the business of IT standards, and view IT systems as enablement mechanisms, which must exist for the actual mission of the organization.

Creation of IT standards by comparison is a process whereby most organizations look to government entities, such as NIST, SANS, and ISC2, and/or use products and solutions, such as Gold Disk, Secunia, and the Microsoft Vulnerability Checker (Many used Gold Disk when it was freely available for download by anyone) to influence security policy and secure actual implementations.

The Framework will provide a good baseline for security and practice

Addressing security from the perspective of IT standards relates back to the maturity of the IT and security organizations, in comparison to the individuals or groups that wish to exploit systems and services operated by these teams. Shrinking IT and security budgets in most industries and verticals means that IT and security teams will be responsible for more services, with less funding to achieve this standard. This heightens the importance of the Cybersecurity Framework, as it will be viewed not only by critical infrastructure sectors, but also by IT providers, as a listing of practices that should be adhered to.

Recommendations for standards

The standards should include logging profiles and log rotation standards, which will provide an organization with insight into what is actually traversing their perimeter, and allow them to address their vulnerability through the use of the security framework's practices. Examining this information forensically will allow any victim to understand the extent of the damage that has been taking place, along with where in the hacking cycle an intruder may currently be operating. An ability to accept various data types and fuse these types of data together into a single, correlated form which can be reviewed for actions and status should be written into the Cybersecurity Framework.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Currently no formal escalation process

In the current environment, many organizations have no formalized escalation process for security events. Instead, the escalation follows an informal process, whereby a senior security engineer or a security officer for the organization is made aware of activities which are of an alerting nature. This lack of process is partially due to the immature cyber structure of many organizations and their budgetary capabilities to address cyber events.

A formal process is needed

A formalized process or standard should exist whereby a defined escalation is distinct, in which a set of events and processes will call for notification to an escalation target. The lack of clear definition in most instances leads to a lack of understanding and further planning, which results in lack of clarity when situations occur.

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

No risks to privacy and civil liberties

Our understanding is that the freedom of speech protection by the First Amendment does not extend to information security. These assets belong to the employer whose public persona may not agree with an individual employee's political or personal views.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

A global policy is not practical

From a global business perspective, implications of this Framework are dependent upon on the countries that the organization is working within, as laws and regulations will vary from country to country. For instance, doing business in countries such as China will result in policies which would preclude certain encryption methods, whereas use of these same encryption methods in Canada or Mexico is acceptable. While application of this policy internationally would be ideal, the possibility of the application of this policy in an international environment is highly unlikely, as it would be remotely effective.

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

No special privilege for privacy and civil liberties when using company assets

Most employers have likely instituted guidelines for privacy involving company or organizational assets which typically stipulate these assets are for business use and any other use is subject for business review. Given this common practice, individuals who utilize organizational assets for any personal business could compromise security within the company network. Privacy and civil liberties while using company or organizational assets should have no special privilege considering the use and subjection to risk the employee introduces to the organization through such use.

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

The importance of cyber analytics

Government organizations and industry alike must look past their competitive nature and security clearances to understand that cyber adversaries are equal threats. To be successful in this struggle, we must share information and develop common standards around safeguarding our nation and our way of life. While the practices listed above are critical in establishing a standard cyber warfare framework, it is equally as important to include a layer of analytics for deeper understanding of potential and future threats. Cyber analytics can provide organizations with enhanced and complementary capabilities, as well as situational awareness about the security of their systems, networks and enterprise. This is realized by monitoring activities; uncovering vulnerabilities, threats and patterns; integrating disparate data; and predicting future threats and attacks so businesses can take proactive measures to protect their data and their networks.

Benefits of cyber analytics include:

- Provides near real-time monitoring that automatically generates attack alerts; at the same time, it dramatically reduces the number of false positives.
- Aggregates, correlates, and merges data from all network monitoring devices and other data sources to provide enhanced network domain and situational awareness.
- Detects and scores the severity of possible attacks before they happen to enable timely intervention measures.
- Provides early recognition of anomalies in network traffic that normally go undetected and uncovers otherwise hidden relationships and behavior patterns that might indicate low and slow attacks.

Discover and extract meaningful

Analytics tools, according to IDC***, “access, transform, store, analyze, model, deliver and track information to enable fact-based decision making and extend accountability by providing all decision-makers with the right information, at the right time, using the right technology.”*** These tools include statistical analysis, forecasting, data mining and operations research, which are used to create an integrated environment for predictive and descriptive modeling, forecasting, process optimization and simulation

Applying analytics to cybersecurity to maximize the value of your data

Analytics can successfully apply the power of statistics and modeling to cybersecurity problems in much the same way it applies to fraud detection, financial management or human resources. Analytics enables users to obtain relevant and useful answers to critical cybersecurity questions, such as:

- From where are the threats and attacks coming?
- How do we assess the likelihood of attacks and intrusions?
- Is there a pattern to the attacks?
- Can we build profiles of the attackers?
- How do we mitigate the attacks?
- Where are our assets concentrated?
- Are we complying with existing security policies?
- How can we do threat analysis?
- How can we create cyber-situational awareness?

A holistic view and a strategic approach

By helping complete a holistic picture of an agency’s systems and networks, analytics can help meet two of the biggest cybersecurity challenges agencies face: coordinating their cybersecurity efforts and producing actionable metrics to quantify the effectiveness of those security efforts. Moreover, instead of just plugging holes and fighting fires, layering analytics will enable organizations to take a strategic approach to prioritizing resources and efforts.

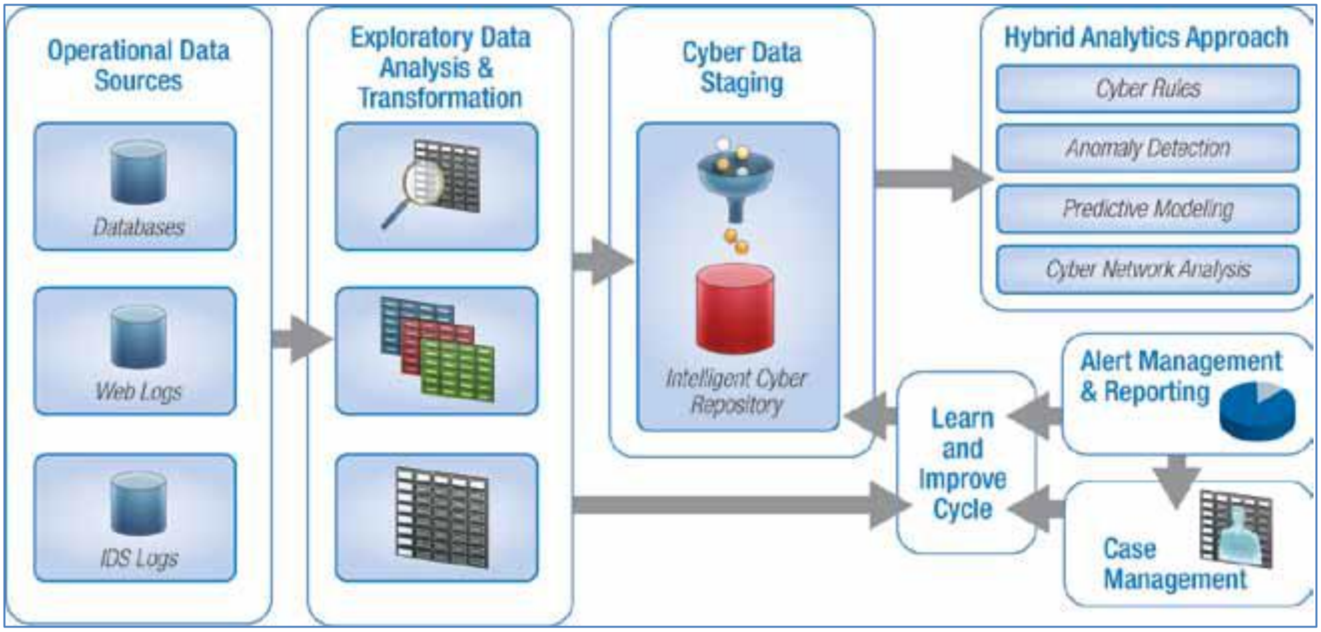

Figure 3: Applying analytics as a cybersecurity solution.

Without incorporating cyber analytics into the nine practices of critical infrastructure, the cyber offenders will continue to finds holes and ways into the network. By utilizing analytics and risk management into the framework, the “system” grows smarter and enables cyber warriors to stay one step ahead while protecting critical assets.