NASCIO
Representing Chief Information Officers of the States

ADVANCED CYBER ANALYTICS:
RISK INTELLIGENCE FOR STATE GOVERNMENT

NASCIO Staff Contact:
Eric Sweden, MSIH MBA
Program Director, Enterprise Architecture & Governance

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States.

Visit *www.nascio.org* for more information on NASCIO

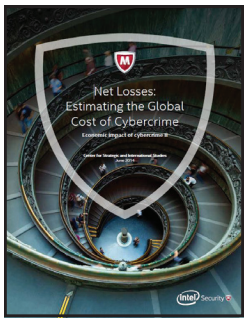
Visit *www.iacpcybercenter.org* for more information on the Law Enforcement Cyber Center.

NASCIO makes no endorsement, express or implied, of any products, services, or websites contained herein, nor is NASCIO responsible for the content or the activities of any linked websites. Any questions should be directed to the administrators of the specific sites to which this publication provides links. All critical information should be independently verified.

This project was supported by Grant No. 2010-DJ-BX-K046 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The stakes are high and unless there are dramatic changes in the way society responds to cyber attacks and deals with cybercrime the losses will continue to exhaust state coffers and strain the economy at a continued alarming rate.

Some estimates present that the impact of cybercrime on the global economy is an annual "leakage" or "hemorrhage" of $375 billion to $575 billion per year.[1] Those estimates do not take into account the aftermath on the lives of those individuals and families working to recover their identities, or restore their losses and to get their lives back or the disruption of government operations and services. Nor do these estimates address the opportunity cost to companies and governments that could have invested these same billions into improving the lives of people in our communities that struggle with poverty or populations that are coping with drought or disease outbreaks or even epidemics; the disruption of government; and lost investments in innovation.



Information has been described by some as

- the lifeblood of democracy,[2]
- the lifeblood of the economy,[3]
- the lifeblood of government,[4]and
- the lifeblood of any organization.[5]

With this in mind, the loss of information can clearly be referred to as a hemorrhage, a drain on democracy, the republic we live in, the economy, government, corporations, and ultimately, a drain on society.

The previously cited report recounts three areas of opportunity cost related to cyber security:

- reduced investment in research and development,
- risk averse behavior by businesses and consumers that limits Internet use, and
- increased spending to defend networks.

Our nation cannot afford these losses or hope the problem goes away. Further, cyber threats are ever changing. Attacks are more sophisticated, more frequent, more effective and more persistent. Advanced persistent threats continue to infiltrate networks and stay there for months or years without the

Key Question:

Who needs to be part of the visioning effort to develop the required foundational intent and motivation across the enterprise?

organization knowing.[6] Too often, the defenses that organizations have are ill suited to today's targeted threat environment with limited integration. This affects our ability to determine the scope of an intrusion and remediation becomes expensive and difficult. The advent of the Internet of Things (IoT) creates a new and lucrative avenue for attack.[7] The number and types of devices is increasing daily. The question being asked regarding IoT and the internet in general is - do the benefits outweigh the potential risks? This report will help frame key issues and recommended actions to attempt to answer this question.

All organizations, including state government, must develop and maintain response capabilities that continuously mature in sophistication in order to keep pace with an ever changing threat landscape. State government remains in a defensive position. Today, it primarily defends, blocks and removes malware, coaches employees on safe technology and information access, and, when possible, prosecutes offenders. With the advent of multi-vector strategies by cyber criminals, state government, now more than ever, needs the ability to correlate disparate data sources generated from the myriad of security tools into which agencies have already invested. States need to continuously update their cyberwar defense portfolio. Some emerging tools will provide new levels of sophisticated capabilities. Other tools will need to be retired due to obsolescence. Most tools will need to be used together in an orchestrated fashion.

Analysts need the ability to have a "single pane of glass" view of all current and emerging threats as well as on-going dialogue with their counterparts and information sharing organizations across the country. That dialogue must also be real-time and *all-time* so that threats encountered by any state or territory, or local government, are shared quickly across the entire state and local government ecosystem.

The attacker ecosystem is continually learning, getting better, improving their operating discipline, and collaborating. State government must do the same. State government does not have the resources to go it alone in this endeavor to protect citizens and government. Successfully protecting state government requires collaboration across states and with federal partners, local government, industry and education. States must continue to mature the cybersecurity ecosystem through collaboration with other communities of interest working together. These include but are not limited to the following:

- state government
- local government
- federal government
- higher education
- K-12 education
- nonprofits
- industry – all sectors
- sector specific information sharing and analysis centers
- critical infrastructure providers: electric, water, natural gas, waste water treatment
- transportation: all modes

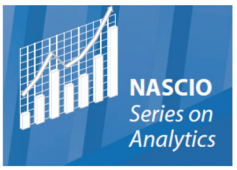
Call to Action:

Understand that information across your entire infrastructure is security relevant

- critical supply chains
- friendly nation states

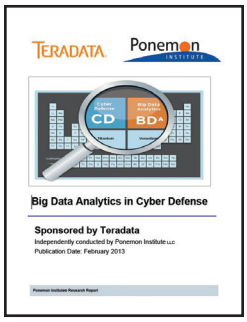
To be effective, this large and comprehensive community will need to mature in detecting and eliminating cyber threats and in sharing actionable information about cyber threats.

What is Advanced Cyber Analytics?



Advanced cyber analytics borrows its definition from business analytics. It is really the application of analytics to cyber security. NASCIO's series on business analytics presents the following definition:

> *Analytics can be described as follows:*
>
> *Analytics is the extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions. Analytics may be input for human decisions or may drive fully automated decisions. Analytics is a subset of business intelligence - a set of technologies and processes that use data to understand and analyze business performance.*[8]



Developing this capability by adding the myriad of available data streams brings us *big data analytics*.

> *Big data analytics is defined as enabling organizations to discover previously unseen patterns and to develop actionable insights about their businesses and environments, including cyber defense.*[9]

Focusing in on cyber analytics we have the following definition.

> *Cyber analytics applies big data tools and techniques to capture, process, and refine network activity data; applies algorithms for near-real-time review of every network node; and employs visualization tools to easily identify anomalous behavior required for fast response or investigation. Cyber analytics tools allow SOCs/NOCs and security analysts to more easily recognize patterns of activity that represent network threats.*[10]

Cyber analytics essentially moves the response from state government closer to the time of the attack, removing as much latency as possible. It includes a growing number of types of tools and capabilities and a new cultural attitude. While network activity data shouldn't be the only data analyzed, it often is. States must acquire and develop a broader range of capabilities beyond network traffic analysis. Canned analytics and rule based analytics will help analysts find some threats - but cyber attacks are becoming increasingly more advanced, and may remain undetected if only using these tactics. As a result, the portfolio of tools is growing. The ability, the tactics, and the creativity in using these tools together is also growing. Some examples of these tools are given later in this report. Further, it can be envisioned that capabilities in

Key Question:

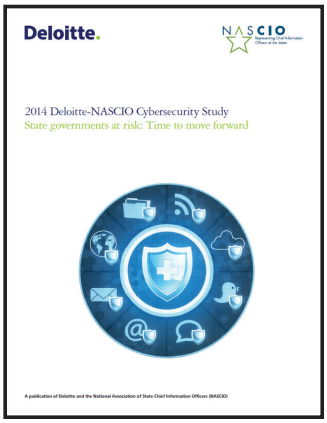
What roles are necessary on a cyber analytics team?

predictive analytics will also mature. Such capabilities move toward predicting and preventing cyber attacks.

Why is it Important?

The game has changed. The threat landscape is on an accelerating curve as presented in the 2014 Deloitte-NASCIO Cybersecurity Study.[11] As described in the study, the types of threats that are arriving over time are not only increasing in number and diversity, but also in sophistication and orchestration. The message presented is alarming and it is clear. Government and industry must develop a proactive, forward looking strategy for dealing with cyber threats if they are going to have any hope of arresting the impact on critical infrastructure and ongoing leakage and outright theft of information from government, finance, healthcare, manufacturing and retail sectors.

The acceleration of cyber threats presents an increasing impact on the business of government. One of the most prevalent concerns today is the proliferation of ransomware; another is cyber terrorism. It can only be anticipated that the accelerating business impact of cyber attacks is juxtaposed with the accelerating motivation behind cyber attacks. Such motivation is based on economical, ideological, religious and political incentives. Such incentives have always existed, but now there is vulnerability that can be exploited. The growing interconnectivity of devices and services can provide an easy on-ramp for cyber attackers to wreak havoc and harm, and gain profit.



Hidden in the acceleration is the increasing motivation and opportunities for exploiting governments, companies and individuals through cyber attacks. It can only be anticipated that this curve will continue to present new and innovative exploitations. Government and industry must develop the discipline, methods and procedures for predicting, anticipating and preventing cyber attacks in advance of these current and future threats.

It is imperative that state leaders realize that it is essential to move forward with investments in advanced cyber analytics. The economic losses and impacts on the lives of citizens are, like the adversary, relentless.

The Lurking Threat of Rootkits

States are at a critical crossroad, either they must invest in increasing advanced response capabilities or lose ground daily in the war against cyber-attacks.

There is a particularly serious concern regarding what some call a *ticking bomb.*[12] Unless states address this concern there will be a series of events

Call to Action:

Share best practices across the cyber ecosystem. Over time grow that ecosystem to include local government, federal government, industry, academia, non-profits, potentially international.

that have high potential for compromising state government operations. It can be presumed at this point that state government systems are infected with a myriad of rootkits that haven't surfaced yet. They are still being traded like the financial markets trade futures.[13] [14] The longer malicious software remains undetected in a computer system, its bid value goes up – it becomes more valuable to the enemies of government organizations. States need to acquire the ability to uncover these malicious intrusions and malware and remove them, neutralize them, and destroy them before they do harm.

Cyber threats are ever-changing, more sophisticated, more pervasive, and capable of wreaking havoc on operations, organizations, and critical infrastructure. States have no choice but to acquire, prepare and exercise new advanced capabilities to fight cyber threats. States have had capabilities such as security information and event management (SIEM) systems for some time. However, existing tools such as SIEM and analytics using visual inspection of network logs are methods within the states' incident response programs that are quickly becoming obsolete. Many such approaches are ineffective and their use almost immaterial by the time malware is identified or data exfiltration is finally discovered.

Capabilities must continually evolve to quickly uncover previously unknown attacks. These analytical capabilities must be deployed and used in such a way as to take account of the business practices and behaviors within the unique business environment employing them. Analyzing all of the organization's machine data allows states to establish a baseline of what can be termed "normal." Then states are positioned to detect and evaluate any deviation from that baseline. Analytical capabilities must be able to learn as business practices change and that normal baseline changes. What may be normal access and network traffic behavior in one organization may prove alarming in other organizations. These adaptive capabilities must be deployed within the context and relevancies of each organization and be nimble to changes that will occur within that organization over time as it adapts and modifies its business strategies and accompanying or supporting behaviors.

What are the Benefits?

Although the use of cyber analytics is fairly new, the benefits of adopting, investing, and deploying advanced cyber analytics are fairly obvious:

- detecting malicious activity earlier
- stopping and reducing the impact of cyber attacks
- preventing data loss and malicious data modification
- protecting data assets, physical assets, workforce and citizens
- assisting in the identification of the attackers
- assisting in forensic investigations in the event an attacker gets through security defenses
- assisting in the prosecution of attackers
- identifying a data breach sooner[15]
- detecting previously unknown attacks, new malicious behavior and insider threats[16] through behavioral analytics

Key Question:

What is the required budget to create a cyber analytics capability?

- providing evidence based approaches through data driven results
- increasing ability to analyze all cyber-centric data and identify statistically relevant data elements

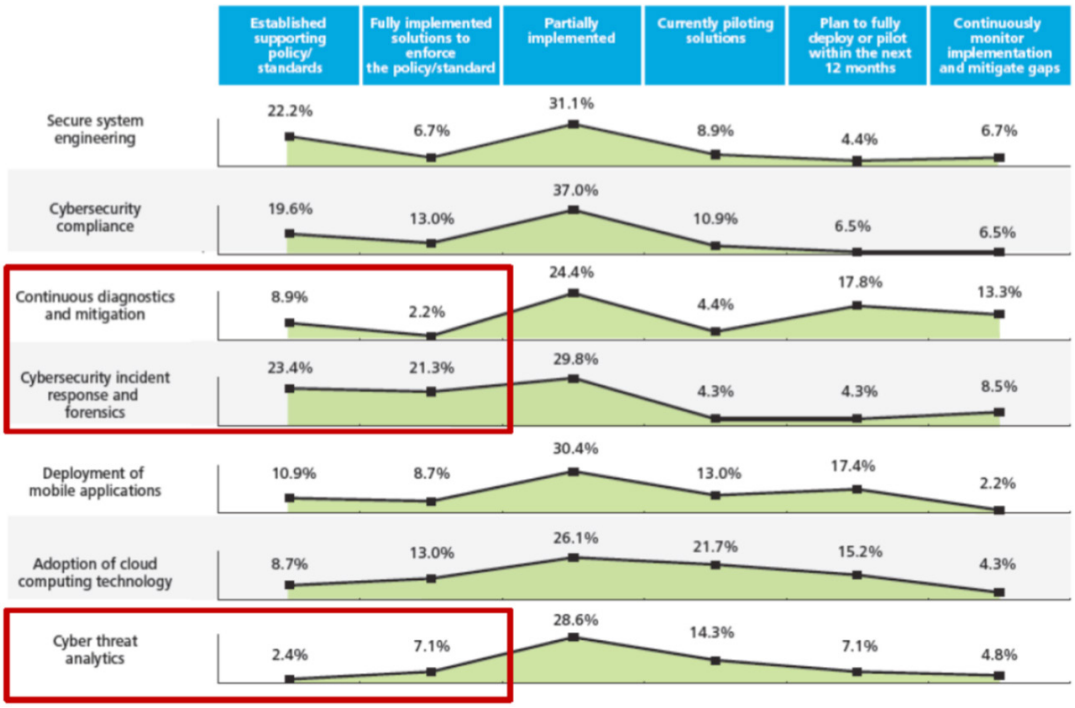
Who is Using it?

Analytics is mainly employed by intelligence agencies or highly advanced industries such as national laboratories and academia. Advanced cyber analytics is currently employed to varying degrees by some local governments, state governments, the federal government, colleges and universities, and corporations. Examples range from local governments like Maricopa County, Arizona and the City of Miramar, Florida,[17] to law enforcement agencies such as the City of Chandler, Arizona's Police Department. Across the states there has been some uptake of these capabilities but as presented in the 2014 Deloitte-NASCIO Cybersecurity Study, there is a long way to go. The results from that survey indicate that few states have established supporting policy standards or reached the fully implemented stage to enforce the policy standard.

There are challenges for most organizations that inhibit adoption of advanced cyber analytics.

- non-analytically mature
- lack of advanced analytics resources – both staff and technologies
- lack of architecture to handle large data volumes
- inability to make the business case for investment
- lack of motivation to purchase next generation tools

"Advanced cyber analytics provides the ability to sift through multiple sources of threat data and respond more quickly. SOC analysts can quickly correlate threat level with endpoint and network events near real time to investigate and mitigate attacks."
Michael Roling, CISO
State of Missouri



Highlights from the 2014 Deloitte-NASCIO Cybersecurity Study

Call to Action:

Establish a real time ecosystem for sharing threat intelligence.

What are the Tools and Capabilities?

There are a number of tools that make up the growing portfolio of tools, techniques, and operating discipline.

- Some tools are more focused on statistical correlation, comparing current traffic patterns, behaviors from specific source IP addresses, data access patterns, outbound traffic variance.
- Some tools incorporate machine learning and artificial intelligence to uncover malicious behavior.
- Some tools are essentially big data analytics engines scouring, sifting terabytes of log file data; rationalizing them down to megabytes and kilobytes that can be further scrutinized for specific known or even new patterns of malicious behavior.
- Tools for testing systems for vulnerabilities.

While all of these different types of tools are essential in collecting data, agencies need to be wary of data silos. Correlating the data from *all* of these systems allows for better threat detection. Beyond the many tools for discovering and evaluating security issues, there are the necessary capabilities for evaluating the events that rise to the surface that need to be communicated across the cybersecurity ecosystem, warning others of potential or real threats.

How Can These Tools and Capabilities be Organized and Evaluated?

Tools: These can be organized and managed as follows:

- those required to carry out individual analytical processes and tasks, support functions and
- those required to provide oversight, management, coordination, and communication.

Benefits: Benefits can be organized similarly as

- individual capabilities, functions, service and
- oversight and management.

Possible clusters of tools which refer to tools that work together or that must be orchestrated:

- Big Data
- advanced analytics
- content analysis
- response and recovery
- social analytics
- predictive analytics
- live memory analytics
- data integration
- fraud detection
- operational and intelligence platforms

Key Question:

What existing business analytics capabilities can be leveraged in developing cyber analytics?

There may be 100 different tools that are being used in a variety of ways and levels of sophistication.
Other examples:

- Semi-supervised Learning
- Cluster Analysis
- Particle Swarm Optimization
- Temporal analysis
- Categorization
- Log management
- Next generation firewalls (NG FW)
- Advanced Threat Services
- Forensics

Advanced Cyber Analytics

At a higher level of abstraction, the capabilities being developed have moved to a higher order employing computers and artificial intelligence to look for abnormalities; surface Trojans; and monitor, evaluate, and neutralize malware, all within milliseconds. The new capabilities in advanced analytics are a new generation from past and even current practices where an analyst is sitting in front of a screen, visually reading through log files. An analyst looking through log files is the *old model*. There are simply too many attacks coming in too quickly and therefore too much time is lost between the initial attack and the discovery of the attack for the old model to be effective.

Today, it must be an intelligent machine doing the viewing, and making decisions in real time. Even if the software is not making the decisions and acting on detected patterns, it can identify and alert on common patterns so analysts can more easily prioritize which log files to evaluate thus providing better focus of limited human resources.

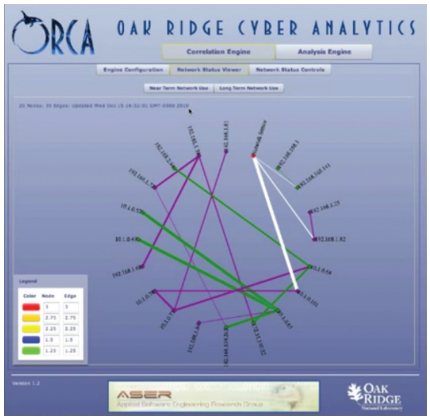
Call to Action:

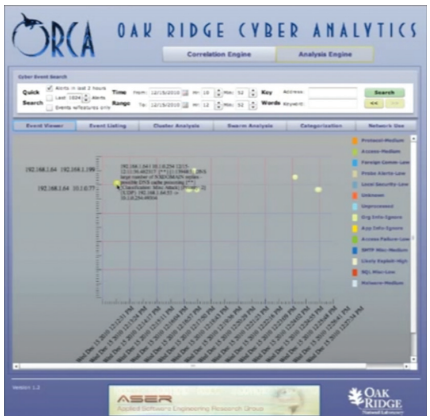
Understand that information across your entire infrastructure is security relevant.

A Few Examples from the Oak Ridge National Laboratory Cyber Analytics[19]

Following are some examples of visual analytics from Oak Ridge National Laboratories. The full view of these examples are cited in the appendix under "Additional Resources." The following images are intended to be illustrative. These examples are fully demonstrated on the presentation cited.

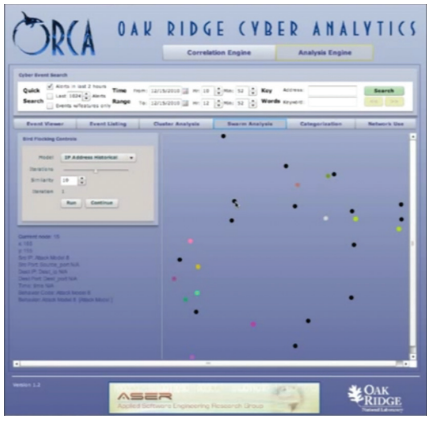
Network use analysis shows the event related communication that has occurred between computer nodes.





Attack behavior modeling is used to identify evolving attack scenarios.

Swarm analysis is a method for evaluating the behavior of alerts with past alerts and uses "bird flocking" simulations to draw affinities between behavioral patterns.

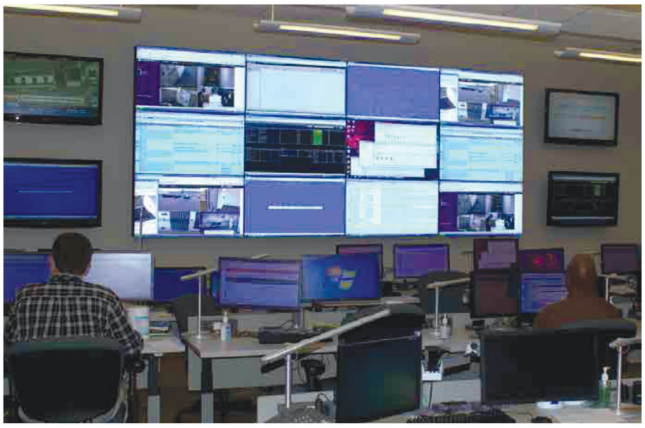


Key Question:

What is the compelling messaging required to gain sustained support from agencies?

Impact on Human Resources and Legal

State governments can rarely afford to hire the necessary number of data analysts or scientists required to effectively use homegrown tools to conduct the required analysis using the old model. Most organizations do not have the necessary skilled staff and can't afford such staff. Advanced cyber analytics requires skilled human talent such as data scientists, statisticians, mathematicians typically at the graduate and PhD level. Cyber analytics platforms can assist with this dilemma. They are designed with security analysts in mind offering canned analytics, an in-built rules engine, and investigation and forensic analysis tools. Employing these platforms can enable a smaller staff to perform at a level that required much larger teams in the past. Training programs must also be put in place to mentor and train existing employees into new roles in advanced cyber analytics. Training should eventually include simulation exercises and development of a cyber range similar to the State of Michigan cyber range for ongoing professional development.[20]



State of Michigan Cyber Range

In the foreseeable future, application of advanced analytics and correlational analysis will result in a percentage of false positives – i.e., something that looks malicious, but isn't. That circumstance will have to be a way of life going forward. We must expect that correlations will have some associated probability or confidence interval. There will always be some level of uncertainty about many types of data patterns that are uncovered.

In addition, there must be operating discipline in place that is precise enough to apply proper due process to acknowledge false positives and exonerate anyone affected. There will be mistakes particularly regarding investigating insider threats. We cannot afford to accuse or prosecute people who are innocent of any maleficence. Auditors and forensic analysts need to ensure investigations don't become "witch hunts," and that there are no incentives for such behavior. Advanced cyber analytics must develop into a profession of the highest integrity. Therefore, it is people of the highest character that must be recruited into this profession.

In many, possibly most cases, unsafe online behavior is essentially the case of employees sincerely trying to get work done. In these circumstances, what is needed is coaching and training. Much of the risky online behavior of

employees and citizens can be, and should be avoided in advance by providing necessary practical training to raise awareness of the intrinsic risks associated with the Internet. Training must include topics such as the risks inherent with open software and free online cloud storage, information classification, and social engineering.

Calls to Action

- Develop a dynamic strategic plan for advanced cyber analytics.
- Create an advanced cyber analytics team that includes the state CIO, the state CISO, enterprise architecture, agencies, strategic business partners, other jurisdictions.
- Understand that information across your entire infrastructure is security relevant.
- Break down information silos and aggregate all of your data in one place.
- Establish a real time ecosystem for sharing threat intelligence.
- Share best practices across the cyber ecosystem. Over time grow that ecosystem to include local government, federal government, industry, academia, non-profits, and potentially international governments.
- Implement a training discipline that ensures all employees are aware of cyber threats including social engineering.
- Establish collaborative relationships across all the agencies so that security experts are consulted and security best practices are embraced by all employees.

Checklist

- ☐ Pull together experts within your organization from data management, data science, business intelligence, data analytics, records management, security, enterprise architecture, enterprise portfolio management and the agencies. Collaborate with this team to develop a vision and strategy for developing a capability in cyber analytics.
- ☐ Working with this same team, develop the economic case for acquiring advanced cyber analytics capabilities. Consult with those states that have already developed such a case.
- ☐ Working with this same team, develop a portfolio of the questions and analysis that will be required of a cyber analytics team. Also, determine the necessary response time required for various types of incidents. That is, based on type of attack, how quickly must the cyber response team act to prevent or mitigate the effects of an event.
- ☐ Consult with other states and local government, industry, academia, and suppliers. Learn what is currently available and what is forthcoming in the way of analytical capabilities and the power of those capabilities.
- ☐ Develop a change management strategy for gaining enterprise commitment. This strategy must include a compelling message for the various stakeholders: top management, policy makers, employees, citizens, suppliers, other jurisdictions, industry partners, regional partners, and law enforcement.

- ☐ Working with stakeholders, determine what training requirements and tools are required to develop capabilities in analytics and specifically cyber analytics.
- ☐ Collaborate with the budget office, the procurement office, supplier-partners, the cyber response team and agencies to develop a budget for supporting, sustaining, and maturing a cyber analytics capability.
- ☐ Develop the necessary ecosystem for sharing advanced threat intelligence. Grow that network over time.

Key Questions

- ✓ Who needs to be part of the visioning effort to develop the required foundational intent and motivation across the enterprise?
- ✓ What roles are necessary on a cyber analytics team?
- ✓ What operating discipline and tools are required?
- ✓ Who is doing this well in state and local government, federal government, industry, and key infrastructure providers?
- ✓ What is the required budget to create a cyber analytics capability?
- ✓ What is the required budget to sustain a cyber analytics capability?
- ✓ What is the compelling messaging required to gain sustained support from agencies?
- ✓ What existing business analytics capabilities can be leveraged in developing cyber analytics?
- ✓ What are best practices and operations for a cyber analytics team?

Recommendations on How to Move Forward with Cyber Analytics

For states that are very early in their adoption of cyber analytic capabilities there are a number of basic investment steps that need to be taken. Some of these steps are supportive steps for enabling advanced cyber analytics. These include, but are not limited to the following:

- Put in place data management operating discipline.
- Create a highly collaborative network of partners and information sharing partners.
- Establish quality management to vet the plethora of analytical tools and then determine what tools should be adopted, which are not ready for prime time, and which ones should be abandoned due to obsolescence.
- Determine how to better leverage tools in which you have already invested. A machine data platform can take data from network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence solutions.
- Establish quality control and other basic management steps and procedures for guiding the strategy and implementation and staging of advanced cyber analytics.

Contributors

- *Erik Avakian, Chief Information Security Officer, Governor's Office of Administration Office for Information Technology, Commonwealth of Pennsylvania*
- *Glen Bellomy, VERITAS Technical Architect, Public Sector, Symantec*
- *Mike Cooke, Web Designer, AMR Management Services*
- *Jen Dunham, Principal Solutions Architect, SAS Security Intelligence Practice, SAS, Inc.*
- *Amy Hille Glasscock, Senior Policy Analyst, NASCIO*
- *Davis Hake, Director of Cybersecurity Strategy, Palo Alto Networks*
- *Bert Hayes, Senior Solutions Engineer, State & Local Government / K-12, Splunk Inc*
- *Sam L. Hearn, Jr., Graphic Designer, AMR Management Services*
- *Christie Hernandez, Field Marketing Manager, Public Sector, Splunk Inc.*
- *Kenny Holmes, CSSP, Account Executive, Palo Alto Networks*
- *Agnes Kirk, Chief Information Security Officer, State of Washington*
- *Emily A. Lane, Program and Brand Coordinator, NASCIO*
- *Kay Meyer, Principal Industry Consultant, SAS Institute*
- *Andris Ozols, NASCIO Special Advisor*
- *Meghan Penning, Membership and Communications Coordinator, NASCIO*
- *Doug Robinson, Executive Director, NASCIO*
- *Renault Ross, Security Business Principal, Public Sector Strategic Programs, Symantec, Inc.*
- *Elayne Starkey, Chief Security Officer, State of Delaware*
- *John Zarour, Director, State & Local Government / K-12, Splunk Inc.*

References

NASCIO
Security and Privacy Publications
http://www.nascio.org/Content/Publications-View/PID/652/evl/0/CategoryID/33/CategoryName/Security

NASCIO Technology Awards
http://www.nascio.org/Awards/SIT

Center for Digital Government
"Big Data and Analytics"
http://www.govtech.com/library/papers/Big-Data-and-Analytics-in-Government-1554.html

HP Security Research
"Cyber Risk Report 2015"
http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

InfoSec Institute
"Cyber Threat Analysis", July 17, 2014
http://resources.infosecinstitute.com/cyber-threat-analysis/

International Association of Chiefs of Police Law Enforcement Cyber Center (LECC)
The Cyber Center is a collaborative project of the International Association of Chiefs of Police (IACP), RAND Corporation, and the Police Executive Research Forum (PERF), and is made possible by funding from the Bureau of Justice Assistance, at the U.S. Department of Justice's Office of Justice Programs.

The Cyber Center was developed to enhance the awareness, expand the education, and build the capacity of justice and public safety agencies to prevent, investigate, prosecute, and respond to cyber threats and cyber crimes. It is intended to be a national resource for law enforcement and related justice and public safety entities.

The Cyber Center addresses three principal functional areas:

- Cyber crime investigations
- Digital forensics
- Information systems security

http://www.iacpcybercenter.org/

FBI- Cyber Shield Alliance
Cyber Shield Alliance (CSA) is an FBI cyber security partnership initiative developed by law enforcement for law enforcement to proactively defend and counter cyber threats against law enforcement networks and critical technologies. CSA encourages law enforcement participation as a force multiplier in defending our national security, while equipping agencies with the training and tools to optimize and defend their own law enforcement networks.
www.iacpcybercenter.org/resource-center/fbi-cyber-shield-alliance/

Multi-State Information Sharing & Analysis Center (MS-ISAC)
The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.
www.msisac.cisecurity.org/

National White Collar Crime Center
For more than three decades, NW3C has worked to support the efforts of state and local law enforcement to prevent, investigate and prosecute economic and high-tech crime. Today, NW3C continues to strengthen this mission by staying current with the technological innovations of the digital age to keep law enforcement up-to-date.
www.nw3c.org/

Oak Ridge Cyber Analytics (ORCA) is a suite of tools for applying automation and advanced analytics to pressing information security problems. ORCA is comprised of several components, each of which addresses widespread technology gaps in computer network defense. The ORCA Development Team is comprised of computer scientists from the Computational Data Analytics group at the Oak Ridge National Laboratory. The team's expertise covers a broad range of techniques associated with intelligent computing.

The ORCA philosophy:

Focus on challenging problems in the cyber security domain for which there are gaps in available technology. The speed, volume, and complexity of cyber security data has outstripped our ability to defend systems with manually intensive processes.

ORCA is designed to provide an adaptive, accurate, and reliable analytic infrastructure for cyber security.
http://orca.ornl.gov/Oak_Ridge_Cyber_Analytics.html

Examples of ORCA's Fusion Engine and Visualizer.
http://orca.ornl.gov/Fusion_Engine.html
https://www.youtube.com/watch?v=EhzXWXl0jSc

Ponemon Institute
"Big Data Analytics in Cyber "
http://www.ponemon.org/library/big-data-analytics-in-cyber-defense?s=big+data

Teradata
"Big Data Integration and Analytics for Cyber Security"
http://www.teradata.com/Resources/White-Papers/Big-Data-Integration-and-Analytics-for-Cyber-Security/

Webinars:
"Big Data and Predictive Analytics: On the Cybersecurity Front Line"
http://www.sas.com/reg/web/corp/2353845

Case Studies:
City of Los Angeles – case study – MeriTalk: www.meritalk.com/csx-profile-city-of-los-angeles.php
State of Alaska - DOA -case study:
carahsoft.adobeconnect.com/_a20595625/p5c6peau0qs.
Nevada DOT – case study: www.splunk.com/view/splunk-at-ndot/SP-CAAAHVU
Chandler PD - case study: www.splunk.com/view/splunk-at-chandler-police-department/SP-CAAAJCV
University of Texas at Austin - case study: www.splunk.com/view/splunk-at-university-of-texas/SP-CAAAG29

---

1 *Net Losses: Estimating the Global Cost of Cybercrime – Economic impact of cybercrime II*, Center for Strategic and International Studies. June 2014. Retrieved on 6/25/2015 from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

2 Silver, H., "Data, Democracy, and Janet Norwood," Social Science Space online network, May 26, 2015, Retrieved on November 2, 2015 from http://www.socialsciencespace.com/2015/05/data-democracy-and-janet-norwood/

3 "Big Data: The Lifeblood Of Today's Economy," *Big Data Week*, April 24, 2013, Retrieved on November 2, 2015 from http://bigdataweek.com/blog/2013/04/24/big-data-the-lifeblood-of-todays-economy/

4 Barrett, K., Greene, R., "The Causes, Costs and Consequences of Bad Government Data", Governing. June 24, 2015, Retrieved on November 2, 2015 from http://www.governing.com/topics/mgmt/gov-bad-data.html .

5 Thuma, T., "Data Is Life Blood: The Ultimate Truth Machine," Forbes, April 23, 2015. Retrieved on November 2, 2015 from http://www.forbes.com/sites/teradata/2015/04/23/data-is-life-blood-the-ultimate-truth-machine/.

6 *ThreatTrends – Threat Landscape Review*. Palo Alto Networks. December 10, 2014. Retrieved on November 5, 2015, from https://www.paloaltonetworks.com/resources/research/threat-landscape-review.html.

7 Donston-Miller,D. , "The Internet of Things Poses New Security Challenges," *Forbes*. February 25, 2014. Retrieved on November 2, 2015 from http://www.forbes.com/sites/sungardas/2014/02/25/the-internet-of-things-poses-new-security-challenges/

8 *DO YOU THINK? OR DO YOU KNOW? Improving State Government Operations Through Business Analytics*, NASCIO, February 2010. www.nascio.org/publications.

9 *Big Data Analytics in Cyber Defense*. Ponemon Institute Research Report. February 2013. http://www.ponemon.org/library/big-data-analytics-in-cyber-defense. p.1.

10 *Big Data Analytics in Cyber Defense*. Ponemon Institute Research Report. February 2013. http://www.ponemon.org/library/big-data-analytics-in-cyber-defense. p.1.

11 *2014 Deloitte-NASCIO Cybersecurity Study – State governments at risk: Time to move forward*, NASCIO, 2014. Available at www.nascio.org/StatesAtRisk. P. 24.

12 From interviews with state CISO and CIO communities.

13 From interviews with state CISO and CIO communities.

14 "Crimeware: Trojans & Spyware," Symantec, Inc. Retrieved on November 2, 2015 from http://us.norton.com/cybercrime-trojansspyware.

15 Current average latency between a data breach occurring and it being detected is 229 days. Mandiant annual threat report, M-Trends, April 2014. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

16 "A Vision for Cybersecurity Detection Analytics," HP Corporation White Paper. Retrieved on July 15, 2015, from http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA5-6876ENW.pdf

17 Case Studies by Fireeye, Inc. Retrieved on November 5, 2015 from https://www.fireeye.com/customers/government-case-studies.html#dismiss-lightbox.

18 Case Studies by Splunk, Inc. Retrieved on November 5, 2015 from http://www.splunk.com/view/splunk-at-chandler-police-department/SP-CAAAJCV

19 Images were taken from ORCA's online demonstration at https://www.youtube.com/watch?v=EhzXWXl0jSc.

20 *Michigan Cyber Initiative 2015*, https://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf