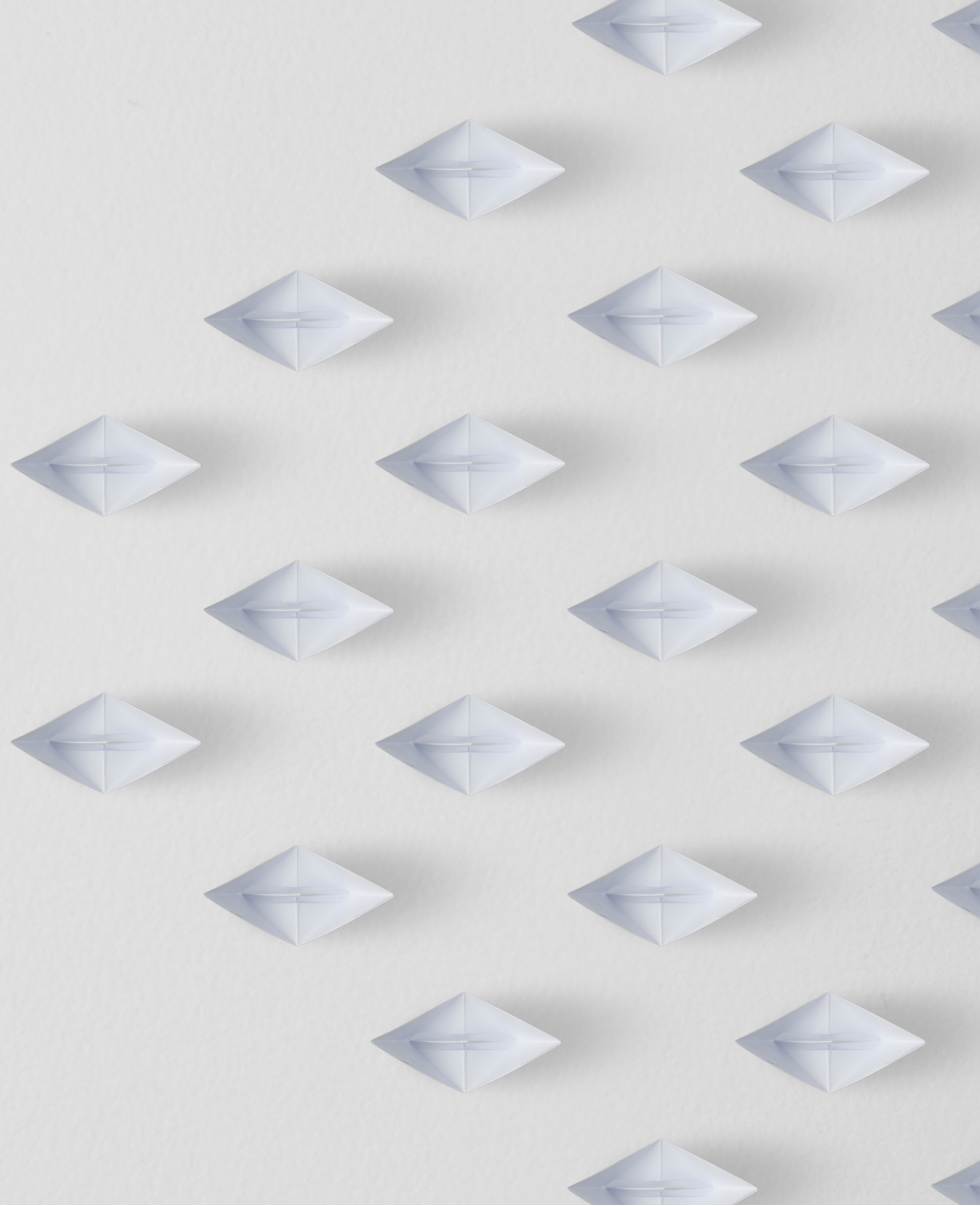
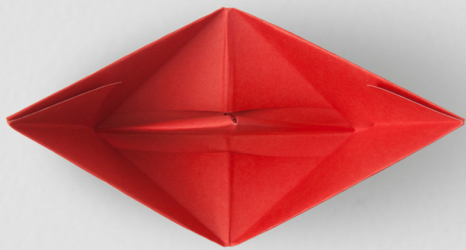


October 2019



MODERNIZATION REQUIRES LEADERSHIP

Leading the way to Cloud Security, Zero Trust, and Threat Intelligence

Authored By:

Don Maclean, ICIT Fellow & Chief Security Strategist, DLT
Parham Eftekhari, Executive Director, ICIT
Drew Spaniel, Lead Researcher, ICIT

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank



Modernization Requires Leadership

Leading the way to Cloud Security, Zero Trust, and Threat Intelligence

October 2019

The authors would like to thank the following experts for their contributions to this paper:

- Peter Archibald, Regional Sales Manager, US Government and Systems Integrators, Checkmarx
- Scott Gordon, Chief Marketing Officer, Pulse Secure
- Alex Gounares, Chief Executive Officer, Polyverse
- Brandon Shopp, Vice President of Product Strategy, SolarWinds

Copyright 2019 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Contents

Introduction	3
Leadership in the Cloud	3
Leadership Focus: Socializing the Cloud	3
The Cloud Can Improve Security.....	4
Service Level Agreements (SLA) and Contracts are Key to Success in the Cloud	4
Cloud Migration Saves Agencies Money, But Tracking Remains an Obstacle	4
Cloud Adoption Mitigates Personnel Issues	5
Zero Trust: Keeping Honest People Honest.....	5
Perimeter Security is Dead, Long Live Zero Trust	6
Leaders Understand that Modernization Brings Greater Access to Data, Knowledge, and Insights	8
Elevating the Value of Threat Intelligence Outside the CISO's Office	8
Conclusion.....	10
Sources.....	11

Introduction

The American government's computer systems are outdated and can no longer defend against modern threats from nation-states, insiders, and organized crime. As Executive Order 13800 of May 2017 states, we must modernize to keep pace with our adversaries. Cloud computing, zero trust architecture, and effective threat intelligence promise to improve the security of government systems.

However, modernization requires investment of time, money, and intellectual capital. Obtaining these requires leaders who can articulate their benefits to policymakers, legislators, agency leaders, and essential collaborators in areas such as operations, procurement, finance, human resources, and privacy.

This paper will discuss the role of leadership in ensuring the success of three aspects of modernization: the cloud, zero trust, and threat intelligence.

Leadership in the Cloud

Years of federal initiatives aimed at creating trust in cloud migration have borne fruit: migrating to cloud platforms is now widespread. Commercial products fit agency requirements and agency executives can make informed decisions about which systems and applications to move to the cloud. "The journeys do not look the same, and that's okay," said federal CIO Suzette Kent at a conference hosted by Docker in May 2019. "It's important that agencies are empowered, based on what they need, to make those decisions." She highlighted examples such as the Department of Justice which has 30 applications in the cloud and stated that in some agencies "as high as 80 percent of what they currently have may be a fit for the cloud," while others may have fewer applications that are suitable for the cloud based on their needs and requirements.

Too often, security decisions are driven by concerns about personnel qualifications, budget, and compliance. Cloud migration can alleviate these problems by reducing burdens on resources and system management. Migrating to cloud platforms enables CIOs and other leaders to ensure strong cybersecurity without sacrificing productivity. Leading cloud applications embed critical security capabilities into their core platform to boost productivity while allowing IT departments to shore up security and reduce management overhead [1]. Proper management of cloud applications improves visibility, network adaptability, and security. For instance, containers reduce the attack surface and can limit the enemy's ability to move laterally to compromise other systems.

Leadership Focus: Socializing the Cloud

The White House Federal Cloud Computing stresses the three key pillars of successful cloud adoption: security, procurement, and workforce. Together, they create an interdisciplinary approach to IT modernization which is needed for the federal enterprise to provide an improved return on its investments, enhanced security, and higher quality services to the American people [2].

When engaging with stakeholders in the early phases of a potential cloud project, CIOs should focus on these critical areas of discussion to build strong support for their project across the organization while simultaneously obtaining the data points necessary to make the right determinations for their agency.

The Cloud Can Improve Security

The Federal Cloud Computing Strategy advises agencies to adhere to risk-based approaches, such as the National Institute of Standards and Technology's Risk Management Framework, when migrating to secure cloud environments. The report to the President on Federal IT Modernization recommended that agencies emphasize "data-level protections and fully leverage modern virtualized technologies." Federal CIOs should explain these concepts in business terms so non-technical business leaders will buy into moving mission-critical systems to the cloud. This includes conversations around zero trust and threat intelligence.

Service Level Agreements (SLA) and Contracts are Key to Success in the Cloud

Educating technical and non-technical leaders on how contracts and SLAs can be used to improve security is an underutilized tool in gaining organizational buy in for cloud initiatives. SLAs increase accountability, clarify security responsibilities, and improve transparency. When contracting a vendor to deploy a cloud solution, agencies must demand a robust SLA and the contract must address key areas such as data location, access to logs, and parameters for notification of incidents, both imminent and ongoing.

Cloud Migration Saves Agencies Money, But Tracking Remains an Obstacle

When adopting a cloud solution, the government struggles with tracking and evaluation of financial savings. Even so, cloud migration has the potential for cost savings by reducing overhead, increasing productivity, and decreasing operational costs. Program managers and CIOs who build precise financial models that convey the short and long-term cost savings for cloud programs, and how those funds can be used elsewhere in the organization, will likely find an audience receptive to exploring cloud-based efforts.

According to a 2017 survey of federal IT leaders conducted by Deloitte and the Government Business Council, the top three reasons organizations move to the Cloud are:

1. Potential cost savings
2. Improvements to operations
3. Sharing and using data in expanded and innovative ways

However, the government's own studies show a need to improve tracking to measure cost savings. According to the April 2019 Government Accountability Office (GAO) report, [Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked](#), over 80% of the audited agencies reported hundreds of millions of dollars in savings after switching to cloud services, but were finding it difficult to track that data. Just under half of the agencies who reported saving money said they had reinvested that budget into other modernization efforts or improvements to IT services.

The Office of Management and Budget (OMB) requires agencies to evaluate each cloud service investment and include that evaluation in their annual budget submissions. However, some agencies reported difficulties assessing these investments in cloud services [3]. GAO attributes these challenges to confusion created by changes in OMB guidance. Since 2015, OMB has changed what investment data needs to be tracked and reported, particularly when cloud acquisitions are included in larger purchases. As a result, OMB staff told auditors “that agency-reported cloud spending data are underreported and the IT dashboard reflects only a fraction of actual federal spending on cloud services.” New guidelines from OMB should eliminate confusion and increase consistency in future audits, as it will require agencies to report total cloud costs by investment. Most agencies agreed with GAO's recommendations to find ways to track savings consistently. However, the Defense Department did not, stating the lack of standard reporting methods renders efforts to collect data on savings and cost avoidance associated with cloud services inefficient and impractical [3].

Cloud Adoption Mitigates Personnel Issues

The government technology community, particularly in the field of cybersecurity, faces multiple challenges in recruitment and retention stemming from a limited pool of candidates, intense competition from other employers, salary caps, and burnout due to repetitive work and understaffing. Migration to the cloud offsets some of the personnel burdens by offloading system management burdens to the vendor and by automating many repetitive processes, leaving personnel able to focus on more value-added processes. Additionally, investment in cloud-based automation tools such as robotic process automation can alleviate the impact of the cyber talent shortage and improve workflow efficiency.

Agency CIOs should engage with Chief Human Capital Officers and business leaders to discuss the positive impact investment in the cloud can have on human resources. In the long term, this may include the development of reskilling programs to ensure employees are trained on new, advanced capabilities as remedial tasks are replaced by cloud services.

Zero Trust: Keeping Honest People Honest

According to Forrester, who pioneered the Zero Trust model, “Cyber threats are prolific and continuously adapting; we are in a cyber arms race where combatants have a broad threat surface to play with and no shortage of tactics to do damage. ‘Trust but verify’ is no longer a valid approach.” Unfortunately, the antiquated perimeter security strategies fail to mitigate threats and allow excessive dwell times for malware.

Adoption of Zero Trust policies empowers CIOs and CISOs to defend against malicious actors, keep honest people honest, and deter unintentional insider threats. According to Forescout, zero trust can be defined as a blueprint for how security teams should redesign their networks, automating security detection and responses, limiting excessive user privileges and access, making their microperimeters secure, and using obfuscation techniques to strengthen data.

The Department of Homeland Security has recognized the value Zero Trust brings to the federal landscape and has established working groups to develop identity, credential, and access management resources in support of Zero Trust [4]. In July 2019, the Department of Defence released [The Road to Zero Trust \(Security\)](#), a publication that detailed how zero trust can improve defense infrastructure, facilitate secure information sharing from enterprises to the tactical edge, and catalyze the adoption of network technologies and enablers, including cloud computing, artificial intelligence, and machine learning. Within a week, the Defense Information Systems Agency launched a zero trust pilot on the Secret Internet Protocol Router Network (SIPRNET) with U.S. Cyber Command [5].

Zero Trust is fast becoming indispensable to a holistic security strategy. When leaders articulate the value of zero trust and secure cloud environments, they speak with authority on the benefits of technology investments and modernization efforts.

Perimeter Security is Dead, Long Live Zero Trust

Perimeter-focused security architectures continue to fail because they default to high trust levels on the internal network. According to researchers from Forescout, “today’s enterprise environments rely heavily on cloud-based services and infrastructure, which effectively erase the network perimeter.” “The zero trust model shifts focus from various types of authentication and access controls, including the fallacy of single security perimeters, to tailored controls around sensitive data stores, application, systems, and network,” says LogRhythm in a related blog. “They leverage identities (in the form of user, roles, and systems) and commission and decommission users and brokers their access based on role. This all sits on top of a network architecture that leverages micro-segmentation, security monitoring and response (analytics, behaviors, automation, orchestration, response, intelligence), and general protective/preventative controls (especially at the device).”

In early iterations, the Zero Trust model focused narrowly on protective segmentation and least-privilege access control; it did not specify how to leverage existing security controls in practical implementations. Over time, the basic model evolved and matured into the Zero Trust eXtended (ZTX) ecosystem. The ZTX framework comprehensively maps relevant security technologies to seven key dimensions of a typical enterprise environment: networks, data, people, workloads, devices, visibility and analytics, and automation and orchestration. Additionally, the ZTX framework helps security teams understand what technology does to:

- Enable the principles of network isolation, segmentation, and security
- Enable data categorization, isolation, encryption, and control
- Protect human users of networks and infrastructure resources, by securing those resources from their users
- Protect workload application stacks in public and private clouds
- Automate and orchestrate Zero Trust controls and processes across heterogeneous environments
- Provide visibility and analyses to illuminate and secure every nook and cranny of the extended enterprise environment

The intended outcome of the Zero Trust model is that trusted identities get role-based access to the applications, systems, networks, and data necessary to perform their jobs. It ensures that trust is verified at every step and that an employee is who they say they are. One Zero Trust strategy is to discover and classify every device that connects to the network, not just those with endpoint agents installed. For each device, a least-privilege access policy is strictly enforced based on a granular analysis of the device, user identity and authorization, software stack, configuration compliance, and security state. To realize such a strategy requires a comprehensive solution for device visibility and control. The system must detect and control hosts that conventional endpoint management systems overlook, such as user-owned devices, corporate endpoints with disabled agents, rogue devices, network switches and routers, internet of things devices, factory floor and other operational technology systems, and virtual machines in public clouds [6].

Zero trust deters breaches by repeatedly verifying the identity of the attacker and denying unauthorized access to systems and data. A compromise of one identity type, such as user, device, network traffic, application, or data, does not constitute a compromise of all identity types. If a user was compromised, an attacker would still need to separately compromise the trust invested in the system, network, and monitored behaviors before the attacker could access restricted data. If a system was compromised, the attacker must still breach the trust of the other types of identities. If any of the identity attributes are inconsistent or risky, CISOs can intelligently respond with additional authentication methods or other compensating controls, such as isolating, containing, or removing the user. This creates a quick way to contain a threat before a catastrophic breach occurs [7].

Transitioning to zero trust is not for the faint of heart, but, for most organizations, the increased security is worth the challenge. For instance, due to the size and complexity of its environments, Google dedicated six years to adopting zero trust. Google was a pioneer of the model, but for many smaller and more agile organizations zero trust implementation will take far less time. CISO and Vice President of LogRhythm Labs, James Carder, recommends the following steps to implementing a zero trust model:

1. Identify your sensitive or toxic data sources
2. Identify roles and assign people to a single role
3. Map the transaction flows regarding the toxic data
4. Design a Zero Trust network based on the toxic data sources and how they are used in transactions
5. Write rules on segmentation or policy gateways, like Cloud Access Security Broker, based on the expected behavior of users and applications
6. Monitor the network, inspect and log the traffic, and update your rules based on your behavior analytics

He also names five key technologies he uses to implement Zero Trust:

1. Identity and access management
2. Privileged access management
3. Cloud access security broker or another policy orchestrator
4. Human resource systems as the recommended single source of truth

5. Security information and event management analytics or another user and entity behavior analytics solution [8]

Leaders Understand that Modernization Brings Greater Access to Data, Knowledge, and Insights

Modern systems can increase access to the vast amount of data stored in federal agencies, and the insights hidden in that data can transform an agency's ability to make business decisions and defend against adversaries. Cyberspace is the new domain of war, as evidenced by prolific attacks in recent years including the \$1 billion 2013 Target breach, the infection of some of America's critical infrastructure with the BlackEnergy malware in 2014 by the Russian state-sponsored Sandworm APT, and the theft of 21.5 million SF-86 forms from the Office of Personnel Management in 2015 by the Chinese state-sponsored Deep Panda APT.

Consider the December 2018 GAO study, [*National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies*](#), which identified 26 long-term threats to US national security within 4 categories: Adversaries' Political and Military Advancements, Dual-Use Technologies, Weapons, Events and Demographic Changes. This publication revealed that virtually every agency holds data essential to our nation's defense. Access to all this data combined would benefit intelligence analysts in developing strategies to defend our nation. We must ask ourselves: how accessible is the data our intelligence analysts need? Can agencies analyze it and turn it into action?

Mitigating threats requires agencies to glean knowledge from their mission-critical assets and recognize adversarial activity. Knowledge is power, and leaders need to "know thy enemy as they know thyself." CrowdStrike's blog highlights the need for threat intelligence collection, analysis, and sharing, stating that "it is critical that organizations have consumable Intelligence so that they can understand the adversary, learn from attacks and take action on indicators to improve their overall defenses" [9]. In 2017, the US Government increased investments into four new strategies to protect its vital infrastructure and secure its sensitive information:

- Proactive cyber-threat hunting
- Increased use and sharing of cyber intelligence data
- Continuous security monitoring, with an emphasis on boundary protection and security event lifecycle management
- Automation and orchestration of security operations [10]

Elevating the Value of Threat Intelligence Outside the CISO's Office

Threat intelligence may not be an obvious talking point with non-technical or non-cyber leaders, and it certainly should not be a major selling point for the value of digital transformation. However, non-cybersecurity executives can understand how improved threat intelligence analyses would benefit any agency's mission, demonstrating the value of digital transformation.

Tripwire's blog recommends discussing threat intelligence by first defining threats according to a combination of intent, capability, and opportunity. They argue that "Many organizations fail to identify threats and thus, usually appropriate security resources to the wrong areas or spend too long on processes, such as risk and vulnerability analysis, instead of mitigating and fixing issues." In other words, failing to understand the threat not only prevents an organization from accurately defending themselves, but also wastes time and money in the process. Tripwire goes on to define a threat according to three distinct aspects:

- Intent is a malicious actor's desire to target your organization
- Capability is their means to do so, such as a specific type of malware
- Opportunity is the opening the actor needs, such as vulnerabilities in software, hardware, or personnel

Threat intelligence is crucial because it helps determine if a threat actor poses a credible threat to the organization. For example, an attacker is not a threat if they have capability and intent, but lack the opportunity to attack.

McAfee defines shared threat intelligence differently, as "[C]urated information about an existing or emerging cyber threat that can be distributed for the purpose of improving defenses against a specific attack. Threat intelligence provides critical context around a threat activity, including indicators of compromise (IoC), indicators of attack (IoA), the tactics employed, and, potentially, the motivation and identity of the adversary."

The ability to leverage shared threat intelligence to search endpoints and actively identify threats is a perpetual process. To discover both the external origins of breaches and the internal compromise of systems and data requires advanced tools, technology, and people. Obtaining and maintaining full visibility of all the threat actors targeting a specific environment is essential for enabling cyber threat hunting operations in complex settings. Internal and external threat intelligence capabilities, established and maintained by security-conscious leaders, are necessary to ensure the appropriate amount of threat visibility is achieved for effective hunting operations within secure networks.

Another impediment to effective mitigation of digital threats is anytime a dearth of collaboration exists across intra-agency and inter-agency silos. Modernization efforts and active leadership from federal agency, policy, and legislative stakeholders creates more information-sharing mechanisms to facilitate this type of exchange.

One outcome of improved collaboration is that the intelligence gleaned from information sharing can be proactively incorporated into IoCs to search for other signs of malicious activity, such as nefarious users who may be harvesting data and performing privilege escalation. Analysts collect and analyze data using frequency of occurrence analyses to better discover anomalies that might have gone undetected by implemented controls. This technique enables analysts to focus on finding deviations in the environment that IoCs did not detect. Intelligence garnered from these hunting techniques is easily codified into the IoCs and used to search for other signs of malicious activity, such as data harvesting and privilege escalation by unauthorized users. These techniques also enable proactive searching for

additional evidence of malicious activity, such as non-targeted and commodity-based malware. Stopping these often prevents damaging consequences [11] [12].

While gathering, aggregating, and sharing threat intelligence is vital, it is not enough to mitigate emerging threats. Bleeding edge technologies such as machine learning and AI-driven anti-malware promise the ability to leverage the collected IoCs and other technical information into learning algorithms that train applications to recognize the malicious activities, even of unknown threat actors, before the system is compromised.

Conclusion

Modernization and digital transformation are crucial developments in the defense of mission critical government systems against nation-state adversaries, insider threats, and cybercriminal organizations. They also offer the benefit of increased efficiency for government agencies. Cloud computing, zero trust, and proactive threat intelligence initiatives are the efforts that promise the greatest return on investment. As discussed in this paper, the key to success in any of these areas is strong leadership. This includes CIOs and CISOs who effectively communicate the value of technological investment to business leaders across their organizations. By focusing on innovation, operational improvements, and cost saving, the public sector will quickly realize the benefits of technological investment and work to improve its ability to deliver services to citizens, business users, and the government.

Sources

- [1] "Government No Longer Has to Choose Between Cybersecurity and Productivity", *Govtech.com*, 2019. [Online]. Available: <https://www.govtech.com/security/Government-No-Longer-Has-to-Choose-Between-Cybersecurity-and-Productivity.html>. [Accessed: 04- Oct- 2019].
- [2] S. Kent, "FEDERAL CLOUD COMPUTING STRATEGY", *Whitehouse.gov*, 2019. [Online]. Available: <https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf>. [Accessed: 04- Oct- 2019].
- [3] C. Gunter, "GAO: cloud saved agencies \$300 million, but data is incomplete -- FCW", *FCW*, 2019. [Online]. Available: <https://fcw.com/articles/2019/05/06/gao-cloud-savings-gunter.aspx>. [Accessed: 04- Oct- 2019].
- [4] "Identity, Credential, and Access Management (ICAM)", *Department of Homeland Security*, 2019. [Online]. Available: <https://www.dhs.gov/safecom/icam-resources>. [Accessed: 04- Oct- 2019].
- [5] L. Williams, "DISA pilots zero-trust networking", *FCW*, 2019. [Online]. Available: <https://fcw.com/articles/2019/07/16/disa-zero-trust.aspx>. [Accessed: 04- Oct- 2019].
- [6] "Total Visibility:The Master Key to Zero Trust", *Forescout.com*, 2019. [Online]. Available: <https://www.forescout.com/company/resources/total-visibility-the-master-key-to-zero-trust/>. [Accessed: 04- Oct- 2019].
- [7] J. Carder, "What is the Zero Trust Model for Cybersecurity, Really? | LogRhythm", *Logrhythm.com*, 2019. [Online]. Available: <https://logrhythm.com/blog/what-is-the-zero-trust-model-for-cybersecurity/>. [Accessed: 04- Oct- 2019].
- [8] J. Carder, "How to approach a Zero Trust security model for your enterprise", *CSO Online*, 2018. [Online]. Available: <https://www.csoonline.com/article/3253571/how-to-approach-a-zero-trust-security-model-for-your-enterprise.html>. [Accessed: 04- Oct- 2019].
- [9] R. Scobey, "Threat Intelligence the CrowdStrike Way", *Crowdstrike.com*, 2019. [Online]. Available: <https://www.crowdstrike.com/blog/tech-center/crowdstrike-threat-intelligence/>. [Accessed: 04- Oct- 2019].
- [10] "Cybersecurity Funding", *Whitehouse.gov*, 2019. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf. [Accessed: 04- Oct- 2019].
- [11] R. Bejtlich, "Will Sharing Cyberthreat Information Help Defend the United States?", *Brookings*, 2015. [Online]. Available: <https://www.brookings.edu/opinions/will-sharing-cyberthreat-information-help-defend-the-united-states/>. [Accessed: 04- Oct- 2019].
- [12] "How Government Agencies are Facing Cyber Security Challenges", *Fireeye.com*, 2019. [Online]. Available: <https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/how-govt-agencies-are-facing-cyber-security-challenges.pdf>. [Accessed: 04- Oct- 2019].