6-2020

PREVENTING RANSOMWARE WITHIN LOCAL GOVERNMENT AGENCIES: A PUBLIC POLICY ANALYSIS PERSPECTIVE

Bruce Cole

PREVENTING RANSOMWARE WITHIN LOCAL GOVERNMENT AGENCIES: A PUBLIC POLICY ANALYSIS PERSPECTIVE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

by

Bruce William Cole

June 2020

PREVENTING RANSOMWARE WITHIN LOCAL GOVERNMENT AGENCIES: A PUBLIC POLICY ANALYSIS PERSPECTIVE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Bruce William Cole

June 2020

Approved by:

Conrad Shayo PhD, Committee Chair

Jesus Canelon PhD, Committee Member

Javad Varzandeh PhD, Department Chair

ABSTRACT

Cases of ransomware within local government agencies have become prevalent over the last decade. While solutions to ransomware are available, local government agencies are slow to implement such measures. As a result, local government agencies are among the most famous victims of ransomware. This project attempts to provide an answer for ransomware prevention within these agencies from a public policy perspective. To formulate this answer, the issues local governments face in combating ransomware are compared to the solutions implemented in the private sector. This project then analyzes the mechanisms local governments have at their disposal to implement such solutions through the public policy analysis process and provides a hypothetical policy agencies can use to combat ransomware. Finally, a real-world case study provides a context of what solutions local governments have implemented and where these agencies are falling short. This project found that policies focused on ransomware and cybersecurity at large are not being developed nor implemented within local government agencies. It is recommended that local government agencies should consider developing and implementing specific policies to combat ransomware and other cybersecurity crimes.

DEDICATION

I would like to dedicate this project to the Rock Scientist. Never give up on your dreams – Dad.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE
BACKGROUND

Malware attacks against government agencies have occurred since the inception of the internet. In the past, most of these attacks were based on two primary, but different objectives. One was the extraction of sensitive data for the personal gain of the hacker who extracted the data. The other was a hacker who was not looking for personal gain, but instead, was looking to disrupt the operations of the government by shutting down their computer networks through a denial of service (DoS) attack.   However, cyber-attacks have evolved, and hackers began using a different mechanism to infiltrate networks. This new type of malware both disrupted services and led to financial gain – ransomware.

In the case of ransomware, an attacker captures a private network, locks down the access or encrypts the data, and only allows the owner to regain access through compensation. Because of the potential significant impact of ransomware, the spread of these attacks has become prevalent. Ransomware attacks have grown 200% since 2014 (Zamora, 2019). Additionally, ransomware is not biased to a particular type of business or agency. Every institution from small businesses and nonprofits to large healthcare companies have fallen prey to ransomware. Of these attacks, ransomware attacks against government agencies have grown exceptionally, only second to small businesses. Ransomware attacks against local government agencies are uniquely troublesome due to the type of sensitive data these agencies contain and the impact it imposes on citizens.

Ransomware attacks against local government agencies present issues that begin in their information technology infrastructure. It is common for many local agencies to face dilemmas in funding their information technology departments. Even more alarming is the fact that they lack the resources to keep the infrastructure they do have up to date. Many chief information officers find themselves parsing scarce resources while sacrificing best practices. Often, information technology professionals inside of local governments discard cybersecurity mechanisms and methods for other more traditional infrastructure needs. However, the current demand for defending government networks against ransomware attacks cannot be ignored. In 2019 alone, 55 local government agencies inside of the United States were victims of ransomware attacks, totaling millions of dollars in damage (Freed, 2019). Ransomware attacks against these agencies potentially have severe consequences as these agencies provide essential services that many constituents depend on every day. Preventing local governments from operating through ransomware has the potential to have negative life-changing effects on many people.

Problem Statement

This project analyzes best cybersecurity practices and mechanisms within the private sector and government agencies in order to provide a solution for local governments to combat ransomware. The focus will be on the following questions:

- What are known best practices for combating ransomware attacks within the private sector that local government agencies can utilize?
- What are the challenges for implementing such best practices in local governments within the United States?
- What are the specific practical solutions available to help local governments combat ransomware attacks?
- What resources can local governments utilize from other aspects of government operations to assist in developing a ransomware prevention policy?

This project will first establish the correlation between the information technology challenges of local government agencies and their targeting as victims of ransomware attacks. Many local governments within the United States face significant information technology (IT) challenges. These challenges include a lack of good IT based infrastructure and the inability to attract skilled employees due to inefficiencies in pay. Additionally, a local government's IT infrastructure is very diverse as these governments perform an array of services to citizens (Evangelakos, 2019). These issues directly relate to why government agencies are being victims of ransomware. Data from a survey at the national level will provide a context of the challenges local governments are facing. This project focuses on the mechanisms, resources, and tools local governments have at their disposal to prevent ransomware, and provides a public policy analysis perspective to develop a policy that effectively combats ransomware that meets or surpasses that of the private sector. Private sector solutions are analyzed to discover resources local governments can implement within their agencies. After this analysis, market-based policies local governments can utilize, such as franchising and public-private partnerships, will provide contracting mechanisms to assist in implementing a ransomware policy.   Public sector financial analysis tools and educational platforms, such as performance-based budgeting, are utilized with market-based solutions, to develop performance measures that will be the foundation of this new ransomware prevention policy. Finally, the project includes a logic model that demonstrates the needs, outcomes, expectations of this policy. The logical model establishes key performance indicators (KPI's) to ensure ongoing policy success.

CHAPTER TWO
RANSOMWARE

History of Ransomware

The genesis of ransomware is modest at best. The first known attack was poorly coded and used essential confidence defrauding techniques to infect victim's computers. Yet, the first known case was very poignant by providing inspiration for future attacks. In 1989, a large number of delegates of the World Health Organization Aids Conference fell victim to the first known ransomware attack. Weeks prior to the conference, these delegates were sent floppy disks with the instruction that these floppy disks contained information about the upcoming conference in Stockholm, Sweden. In actuality, these disks had a Trojan horse that dispersed a worm in the user's MS-DOS based PC. After the initial infection, the worm would replicate itself each time the PC was turned on and the 90th time, the PC became locked. The locked-down of the user's PC was very reminiscent of modern-day ransomware attacks. This attack would become known as the AIDS Trojan attack. Upon the lockdown of their PCs, users were shown a lockdown screen stating that their PC "lease had expired," and payment of $189 was to be made to a lockbox in Panama City. Again, not that all different from the attacks we experience today. This attack did have one fundamental flaw; the code was generic, resulting in poor encryption. Security professionals were able to decrypt the code quickly, which resulted in very few people paying the ransom. Nevertheless, the attacker succeeded in planting the seeds of ransomware for future generations.

After the Aids Trojan attack, ransomware nearly went dormant for the next decade. It was not until 2003 that a prominent ransomware attack appeared. The 2000s was the height of peer-to-peer file-sharing programs. Millions of files during this period were shared through these platforms, which provided a perfect resource for the deployment of ransomware attacks. In these cases, hackers would embed code in the files being shared, very commonly MP3 or MP4 based files, which, once downloaded, would infect the victim's computer with a form of ransomware. Since these file-sharing platforms were technically illegal, attackers would alert the user that they had been caught illegally sharing proprietary music, videos, and software. The message would state that the user was required to pay a fine to avoid imprisonment. This technique is not very different from the false debt collection phone calls scams during the 1980s, only in digital form. These attacks proved successful, as many of the victims would wire the money or use a credit card to pay the so-called fine (Palmer, 2019). It is essential to emphasize the simplicity of many early ransomware attacks.   Many cases were merely extensions of previous mail and phone-based scams that used intimidation and threats to seize money from victims. However, initial ransomware attacks were, in fact, successful, and provided the crucial groundwork for future attacks. This inspiration has led to the modern-day ransomware attack – attacks that are more devastating and costlier to its victims.

Ransomware Methodology

Popular file-sharing programs of the 2000s mainly drove ransomware attacks. These incidents became the baseline for the modern-day ransomware attacks, and cybercriminals took notice. Since 2010, several current based ransomware events began to occur. Similar to previous events, these attacks use social engineering to infiltrate the user's computer, typically through email phishing or false links embedded into webpages. Modern ransomware attacks are classified into two distinct methods on how they infect a computer or network. One is a direct download rootkit-based method. Most commonly, the malware is disguised as an email attachment.   This rootkit based attack, in most cases, hides within the operating system. Once rooted in the operating system, the ransomware program triggers after a sequence of events; usually the number of times the computer is booted, or an application is launched such as Microsoft Outlook. It is important to note that ransomware behaves differently than other rootkit malware. Rather than wanting to hide itself to remain undetectable, ransomware intends to make its presence known. Once deployed, the ransomware program encrypts the user's data or locks access to the computer. The user is then prompted for payment in order to regain access.

The other form of modern ransomware is a communication-based bug. Rather than embedding the ransomware program in a user's operating system, the malicious link instead starts communication to a landing page for an exploit kit (Johnson, 2016). The server the exploit kit is on starts retrieving information about the software versions the victim is running and identifies vulnerabilities. The malicious program will scan for an unpatched or outdated version of the operating system or other embedded software to identify a way to penetrate the user's computer or network. After the vulnerability is identified, the server pushes down the malicious program. At this point, this method essentially becomes a rootkit and hides itself and its trail within the operating system. The result is the encryption of the user's data and demand for payment to restore access.

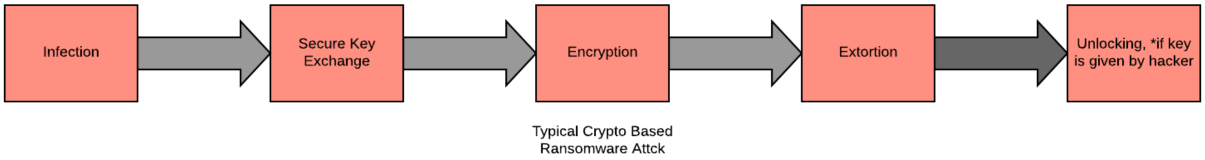

Infection
Secure Key Exchange
Encryption
Extortion
Unlocking, *if key is given by hacker
Typical Crypto Based Ransomware Attck

Figure 1. Ransomware Process

The behavior of ransomware can be classified into three categories: locker, crypto, and hybrid (Ahmed et al. 2019). Locker, as the name suggests, locks the entire device at large. In the case of these types of attacks, the data files on the victim's computer or network are not modified as this type of ransomware specifically blocks access functionality. Crypto methods infect and encrypt specific files on a computer or network rather than the entire device. Crypto attacks target specific files typically through the asymmetric encryption process by denying the user access to the public key (Ahmed, et al, 2019). Hybrid-method based attacks combine aspects from both crypto and locker by encrypting target data and locking access. This type of attack has become particularly troublesome for IoT devices connected to networks as it can compromise both backend and front end based devices (Ahmed, et al, 2019). There is, however, a fundamental and significant difference between the crypto and blocker methods of ransomware. Blocker methodologies, in many instances, can be reversed by reloading a computer's operating system. In most cases, the files on a computer have been backed up, and simply restoring the operating system can regain access to these files. In contrast, crypto and hybrid methods specifically encrypt files, thereby making them impossible to recover without the key.

Ransomware Current State

Ransomware, like other forms of malware, are not static within their programming and function. Several strains of modern ransomware have taken prominence over the last decade and these strains continue to evolve based on newly discovered vulnerabilities in an array of software and firmware. One could argue that the most prolific and impactful strain of ransomware ever created was Wannacry. The Wannacry outbreak began in May of 2017, where several European countries fell victim to this network-based attack. Within the Windows server message block (SMB) protocol, the protocol that allows for the sharing of files and other data on Windows-based PCs and servers, a group of grey hat hackers from the National Security Agency found a vulnerability known now as Eternalblue (Jones, 2017). The basic premise of the Enternalblue exposure is the ability for a potential hacker to inject a shell within the communication during SMB communications. This action allows for the malicious Wannacry code to affect a PC or server. Wannacry, contrary to initial beliefs, was not spread by malicious email or other social engineering techniques, but rather by a piece of poorly written code within a commonly used protocol. Unknown sources leaked the discovery of Enternalblue to a group known as the Shadow Brokers, who then dumped the exploit across the internet. The first case of Wannacry occurred just two weeks after this dump (Jones, 2017). The SMB exploit that allowed the Wannacry pandemic to occur was based on old code that was patched by Microsoft months before the vulnerability was publicly known. Wannacry was only successful against PCs and servers that were not up to date on security patches. Several European local governments were behind on their network patching (Jones, 2017). All governments, from small special districts to large state governments, should use the Wannacry case study as a fundamental reason to maintain all software updates security patches.

Wannacry, however, is certainly not the only strain of ransomware to affect local governments. In fact, inside of the United States, Wannacry was not prevalent among government agencies (Jones, 2017). Nevertheless, other strains were very successful in penetrating government agencies. Another popular type of ransomware was the SamSam bug that took advantage of vulnerabilities within the JBoss servers' open-source platform. In March of 2018, employees of the City of Atlanta started to notice that certain public-facing applications were experiencing outages. Public web portals, such as an application for citizens to pay their water bills, was suddenly unavailable. One by one, outward and eventually inbound facing applications starting to go offline. The applications instead prompted a message asking for Bitcoin payment for the City of Atlanta to regain access to their files and applications. The City of Atlanta had become a victim to relative old nemesis in terms of ransomware, the SamSam bug (Hoffman, 2018). By March 2018, the SamSam bug had, in fact, already infected numerous local governments, including the Port of San Diego and the State of Colorado.   In total, SamSam is responsible for effecting over 50 governments within the United States (Hoffman, 2018). SamSam utilizes a vulnerability within JBoss servers' remote desktop access functionality. This vulnerability was discovered in 2015, and patching for the vulnerability was made a short time after. However, many local governments failed to comply with updating their servers, which made them prime potential victims for SamSam. In the many cases of SamSam infecting local governments, many were unable to maintain their security patching primarily due to their lack of information-based technology resources (Hoffman, 2018).

Both SamSam and Wanancry, along with numerous other ransomware strains, infect computers and networks based on software vulnerabilities, typically due to outdated versions of the software. However, new forms of ransomware enhance the method in which it infects a computer or network. This form of ransomware brings the vulnerability to the system allowing the ransomware to infect. This strain of ransomware is known as Robbinhood. Robbinhoom is considered by many network security experts to be the most devastating form of ransomware in use (Brandt, Loman, 2020). Robbinhood is clever, before penetrating a network, it delivers a driver for a commonly used motherboard for Windows-based products, both PCs and servers. This authentic and digitally signed driver is recognized by the Windows operating system, which then installs the driver. Once installed, the PC or server is now open to the Robbinhood attack, an attack that has devastated many local governments. The City of Baltimore fell victim to the Robbinhood bug in May of 2019. In this case, the attacker asked for $80,000 in Bitcoin in order to obtain the encryption keys. City Officials refused, and the attackers were not paid. However, the City of Baltimore has spent more than $18 million in remediation costs, and most data was not recovered (Sussman, 2019). It is important to emphasize that his particular attack was not because of a lack of IT-based resources that resulted in outdated systems with vulnerabilities. This attack was possibly due to the City not having adequate personnel versed in cybersecurity or a cybersecurity team. This lack of talent within local governments is common (Freed, 2019). A cybersecurity professional within the City of Baltimore, one could argue, more than likely could have potentially prevented this attack or at least mitigating a substantial amount of the damage.

CHAPTER THREE
RANSOMWARE CHALLENGES AND SOLUTIONS

Local Government Challenges

Many local government agencies face challenges in combating all types of malware, including ransomware. However, it would be misclassification to state that local governments have not utilized practices and policies to prevent these threats. Current policies and procedures include concepts that range from technological infrastructure to employee education programs. Furthermore, local governments in the past have received support from higher governments. The Federal government has been guiding local governments in the area of cybersecurity, which included ransomware prevention since 2012 (Richardson, North, 2017). Therefore, it is evident that many agencies have implemented policies to combat ransomware, but many, if not most, fall short of the need (Norris, Mateczun, Joshi, Finin, 2018). To convey this fact, most information technology leaders within local governments find the current policies and procedures are in drastic need of improvements (Richardson, North, 2017).

It should be emphasized that cybersecurity demands are very fluid, and as a result, many local government agencies fail to keep up. These agencies face significant obstacles to properly secure resources and implement policies that meet the dynamic needs of ransomware prevention. These obstacles, as provided by Richardson and North (2017), include:

1. Inability to staff cybersecurity and information assurance professionals due to inefficiencies in pay.
2. Lack of funding for new information technology infrastructure, which leads out of date technology.
3. The diversity of the support that Information Technology professionals must provide to government
4. The enforcement of policy and practices.

The above obstacles have led to many challenges in combating all types of malware for local governments, including ransomware. While there are a large number of challenges currently affecting local governments, we will focus on three significant challenges that the policy solution will address. It should be noted, data from the National Association of State Information Officers (NASCIO) cybersecurity survey provided contextual data for these challenges. This survey is released on a bi-annual basis to information technology professionals from SLED (state, local, educational, special) government agencies within the United States and asks specific questions in terms of the current cybersecurity issues these agencies are facing. This survey was last issued in mid-year, 2018, and a summary of the data will be provided in Appendix (B).

Challenge 1: Budgetary Control

All local agencies, including school districts, are mandated to budget using line item methodologies (Shah, 2013). The primary motivation behind a line item based budget is to give the same amount of weight or consideration to each expenditure. The idea being that each expense should be objectively analyzed to determine which have the most considerable impact to the budget. There are additional internal control and risk management advantages to line-item budgeting. Government agencies are allocated a specific amount for each expense and cannot exceed this amount, which is legally approved by their elected body. From an accounting and financial standpoint, line-item budgeting reduces risk compared to other budgeting methodologies, which is why all government agencies within the United States utilize line-item budgeting (Shah, 2013). There are, however, drawbacks to line-item based budgeting. First, this process is, in fact, very bureaucratic and time-consuming.   Line item budgets are allocated on an annual basis, which results in a typical budget preparation cycle of 6 months (Shah, 2013). The budget preparation cycle results in the competition of expenditures and expenditures being collated together.

In terms of information technology expenditures, including policies and infrastructure, line-item budgeting requires that information technology leaders justify each level of expense to their elected bodies, which often results in information technology leaders commingling their costs together (Caruson, MacManus, McPhee 2012). As an example, cybersecurity needs could be combined with other network-based expenses resulting in funds needed for cybersecurity being used for different requirements such as new switches or network storage devices. The solution to this is simple yet challenging to implement. Make cybersecurity-related expenses an actual item on the budget. By doing so, all money allocated to that line item must be an expense for cybersecurity needs.   By having this legally mandated funding, cybersecurity-related policies such as ransomware prevention would have the needed funding. This challenge alone is a fundamental reason why local governments face serious cybersecurity challenges (Caruson et al., 2012). According to the NASCIO survey (2018), only 2 percent of local governments' budgets contain cybersecurity line items. A probable reason for this is bureaucracy, while the chief information security officer is advocating for cybersecurity needs, the network manager is advocating for network needs (Caruson et al., 2012). The policy solution presented in this paper looks to address this issue.

Challenge 2: Acquiring Cybersecurity Talent

The acquisition of cybersecurity talent presents two interesting issues to local government agencies. The first is the local government's financial capabilities to hire information and cybersecurity professionals. The other is a local government's competence to outsource their cybersecurity needs to companies who can provide these services. Both issues result in local governments not having the human capital to combat all types of cybersecurity issues, including ransomware.

The attraction, employment, and retention of information and cybersecurity professionals present an interesting problem for local government agencies. Most, if not at all, cannot offer potential employees' salaries that compete with the private sector (Norris et al., 2018). This lack of funding begins at the budgetary issues discussed earlier. When information security policies and programs are not funded directly through a line item expenditure, they cannot request specific positions for those programs (Caruson et al., 2012). Furthermore, the high-level salaries offered in the private sector are something that is just not feasible for many public agencies. When discussing this issue, it is important to note how most local governments are funded – through direct sales tax and special revenue fees. Direct sales tax and special revenue fees are highly susceptible to economic trends (Shah, 2013). Meaning, when there is a downturn in the economy, these agencies are significantly impacted. Due to this, most local government agencies do not have revenue streams that are consistent enough to offer large level salaries.

The other prominent issue in acquiring cybersecurity talent relates to contracting and outsourcing. It is common for small level agencies, defined as having 100 employees or fewer, to outsource most of their information technology needs (Caruson et al., 2012). Since many agencies do not directly fund a cybersecurity program in their budget, we again find that this scenario leads to a competition for priorities. Most agencies contract with a "lump sum" vendor who provides an array of services, which may or may not include cybersecurity

(Caruson et al., 2012). Additionally, many of these agencies have issues in their contracting processes, which is also a budgetary issue. When an agency does not directly fund their procurement programs, they do not have the resources to procure services adequately (Kamensky, Morales, 2013). As a result, these agencies do not use the mechanisms and tools they have at their disposal. These tools include competitive sourcing and public, private partnerships. These tools will be utilized in the policy solution proposed in this paper. This issue is additionally conveyed in the 2018 NAISCO survey. Only 38% of local government agencies used outsourcing mechanisms.

Challenge 3: Cybersecurity Education of Employees

In most cases, ransomware infection begins through a malicious download attached to an email or through a corrupted link. Typically, this is the result of some social engineering where the user follows the link or downloads the attachment with good intentions. For local government agencies, this means employee actions are the genesis of ransomware infections. Unlike other forms of malware, ransomware is a direct result of an employee not appropriately behaving while on the agency's network. Different types of malware, such as a Trojan horse base rootkit, are the result of a hacker deliberately trying to infiltrate private networks through circumventing firewalls and other security-based hardware. Local government agencies must implement educational programs so that employees know how to recognize potential ransomware attacks. However, many local government agencies have not implemented such measures, and those that have been implemented often fail to fully impact the entire organization (Caruson et al., 2012).

Internal employee training needs are essentially divided into two categories, preventing the intrusion from actually occurring and what actions need to be taken if a breach occurs. Local government agencies are falling short in both of these areas. Both Caruson et al. (2012) and the NAISCO survey (2018) indicate that less than half of local government agencies have implemented cybersecurity based education to its employees. The NAISCO survey (2018) and Norris, et al. (2018) provides additional insight into the type of training being implemented at these agencies.   Of the training being provided, 78% of agencies piece their cybersecurity training together. In these cases, the type of attack is not differentiated or what to do when a breach occurs. This lumping of training is likely the significant reason why this training is ineffective; it is merely trying to cover too much information (Norris et al, 2018).

It should be emphasized that ransomware is a unique type of malware that can be prevented mainly by employee actions. As such, local government agencies need to develop training that is not only effective but also incentive-based. While cybersecurity training is mandatory in most cases, employees are typically not tested, nor are incentivized to learn the material (Norris et al, 2018). Additionally, the NAISCO survey (2018) indicates that only about 28% of agencies include risk assessment and response training, meaning that employees are not given the entire scope of cybersecurity.   To resolve these issues, a local government agency’s cybersecurity training, including ransomware prevention, must be all-inclusive and have mechanisms for employees actually to learn the material. The proposed policy solution will provide solutions to these issues.

Ransomware Solutions

Local government agencies do have specific barriers in combating all types of malware, including ransomware. However, when analyzing the impact of ransomware against local government agencies, it is essential to emphasize solutions that do exist. The private sector provides these solutions. According to Richardson and North (2017), three solutions to ransomware prevention are proven mechanisms in the private sector. These solutions include the backing up of all data by a standard like that of the private sector,   the avoidance of emails with embedded links and attachments, and ensuring that operating systems and all related software remain up to date. Each of the solutions directly relates to the ransomware infection methods previously discussed. Additionally, Evangelakos (2019) expands these areas to include practices that treat each incoming attachment, as it could be a potential attack. It is vital to understand each of these areas when developing a ransomware prevention policy.

Data Backup

The first line of defense against a potent ransomware attack is the backing up of sensitive and crucial data. If IT professionals consistently back up their data, then there would not be a reason to pay the ransom during a ransomware attack (Richardson, North, 2017). Local governments, as part of their standard networking policies, do typically implement back up procedures. In most instances, these backup policies include redundancies to ensure more than one back up in the case of data loss. It is a common practice for these backups to remain on the internal network utilizing RAID and SAN devices, which means that the data backup is still on the network (Richardson, North, 2017). In some cases, ransomware encrypts the entire internal network meaning that data recovery is impossible. Further, Caruson et al. (2012) found that many local agencies do not back up their data frequently enough. Local government agencies should strive for data backup policies that replicate private sector practices. Finally, these agencies should procure infrastructure as a service (IaaS) for the backing up of crucial data in a cloud environment (Evangelakos, 2019).

Avoidance of Emails with Embedded Links and Attachments

As previously stated, email phishing and social engineering-based attacks are the most common method for ransomware infections. In the case of local government agencies, this infection is a direct result of an employee downloading a corrupted attachment or following a malicious link delivered by a hacker via an email. Additionally, ransomware attacks have occurred within local governments when a user that is not an employee follows a malicious link (Norris et al., 2018). Commonly, this happens when a user accesses the internet from a public computer on the agencies' network, such as at a library. These two infection methods require solutions that are both educational and technology-based. Again, the private sector provides mechanisms for these solutions. We know that many local government agencies face significant challenges in providing meaningful and impactful cybersecurity education. This is primarily because these programs are not incentive-based at these agencies. The educational policies of local governments are in exact contrast to what occurs within the private sector. It is common for many private companies, especially large-scale companies, to capture highly sensitive data and incentivize employees in cybersecurity education (Richardson, North, 2017). These incentives are not purely monetary based. Instead, they are instruments that provide employees with certifications that assist them with internal promotions within the company or allow them to take extra leave time. It should be noted that these programs test the employees in training to determine their competence level. This practice does not occur within the public sector (Caruson et al., 2012). While the cybersecurity training is mandatory in many instances within local governments, this training typically does not have a testing component. The other solution is technologically based. This solution includes the implementation of intrusion detection systems (IDS) and intrusion prevention systems (IPS) that are configured to detect and prevent emails with malicious attachments and links. This solution requires two main components. One is the equipment itself, which is a challenge for many local governments. As the NASCIO (2018) survey points out, cybersecurity only accounts for 3% of local agencies' budgets. The other component is the personnel to implement and manage the IDS's and IPS's. These highly skilled personnel require a significant level of pay. Many private sector businesses outsource this service, and local governments should utilize this approach as well. The method for the local agencies to do so is covered in the policy solution presented in this paper.

Frequent Patching of All Operating Systems

Ransomware’s modus operandi is to penetrate a network through a flaw or vulnerability of an operating system or software. This method is by far the most prevalent for ransomware infections. In many cases, this vulnerability is known, and the software developer has released security patching. Ransomware hackers are constantly analyzing when well-known software companies release security patching and then footprint for networks that fail to deploy this patch (Ahmed et al, 2019). Therefore, there is a valid argument that the most massive deterrent to ransomware is keeping all essential software up to date. It also seems like a simple solution and one that is easy to implement. However, as previously discussed, local government agencies are failing to keep operating systems or other valuable software up to date. Our first inclination for this issue comes from the NASCIO survey (2018), which found that almost 50%

of local governments are understaffed in their information technology departments.

Further, this understaffing of cybersecurity personnel is not a recent trend. Caruson et al. in 2012 concluded that the majority of local government agencies were understaffed. Meaning, the workforce does not exist to keep vital software up to date within these agencies' networks. Moreover, underfunded information technology departments often mean that cybersecurity programs are nonexistent. Similar to the education challenge previously discussed, this issue is in exact contrast to what occurs within private-sector practices. Private sector practices to prevent ransomware include an information assurance policy that guarantees the frequent patching of all software (Richardson, North, 2017). In instances where internal cybersecurity personnel do not exist within the organization, it is common to outsource these services. Local government agencies need to utilize mechanisms, such as outsourcing, to ensure that information assurance practices are in place, which guarantees frequent patching.

CHAPTER FOUR
PUBLIC POLICY ANALYSIS

Public Policy Analysis Process

This project has covered ransomware and why local government agencies are vulnerable to these types of attacks. The project additionally covered known ransomware solutions and the challenges in implementing these solutions. The intent now is to develop a policy that local governments can utilize in combating ransomware. Before creating the policy, the public policy analysis process should be explained to show how the context of the policy will solve this issue. There are three fundamental principles of the public policy process, which are identifying the problem, the instrument used in the policy to correct the problem, and the overall goal of the policy. If you know these three things, then you understand the policy. Of course, the actual public policy process is quite complicated and is incremental to implement. When designing and implementing public policy, a policy analyst will follow five steps to ensure the policy's success. Each step is crucial to the development of a ransomware prevention policy.

Step 1: Problem Definition

Problem definition is the most critical step in the public policy process. This step must include the entire depth of the problem definition, which will then shape the actual response. If a policy analyst fails to define the problem adequately, the policy will likely fail (Heineman, Bluhm, Peterson, Kearny, 2011).

It is essential at this step to also understand what the problem is in the realm of public policy. Hoppe (2018) defines a public policy problem as a discrepancy between a real-world situation and the desired outcome. As an example, in identifying the poverty problem, the real-world situation is the millions of Americans living in poverty, and the desired outcome are these people being given the tools to overcome poverty. The discrepancies, in this case, are the numerous reasons why people are living in poverty. Once the problem has been identified, the next step starts with a few basic questions about the problem. These include, when does the problem occur, who does it affect, why is it occurring, and where is it happening? It is crucial to point out that these fundamental questions become very complex, meaning the answers to these questions usually lead to other problems. In using the example of poverty again and answering: “why does it occur?” It can be argued that the lack of education can lead to poverty. So defining the problem of poverty has also become a problem with education. This process is known as problem "clustering." This process is expected in the public sector because most problems that the government is trying to solve are involved, meaning that one problem is usually the result of other problems. This issue is solved by issuing framing, which is the process of identifying all viable stakeholders, origins, and costs of the problem (Hoppe, 2018). The process of issue framing begins with problem clustering, and if done well, it will lead an analyst to all known sources within a problem.

Step 2: Instrument Design and Analyst

Once the problem has been adequately defined, the next step for the analyst is deciding how to solve the problem by designing the instrument. Typically, policy analysts design instruments based on the desired outcomes, which are usually based on altering or changing a behavior, changing economic, political, or social conditions or providing a service (Hoppe, 2018). In this regard, policy instruments are based on what governments have the power to do. Peters (2016) finds that governments usually base their policies on a direct provision, tax, subsidy, regulation, and authority. Typically, most public policies include one or more of these types of actions. As an example, a ransomware prevention policy may consist of a new information assurance regulation as well as a new tax to fund the policy. At this step, the policy analyst examines the well-defined problem and chooses the action to take by selecting the government's authority and the desired outcome. This step is all about choosing the correct instrument. The problem in this regard will shape the instrument, and the policy analyst must consider the instrument's outcome. As an example, a regulation requiring businesses to donate a portion of their profits to help combat poverty would not be an excellent instrument to use as this could entice businesses to leave the government’s jurisdiction, but offering tax subsidies to companies to donate to charity will probably entice businesses to do so.

The issue at this stage of the public policy process is based on intended outcomes. The solution to this issue is instrument analysis. This is important because some instruments may have negative outcomes. Peters (2016) stresses that a policy analyst must analyze all possible instruments to determine all possible results at this stage. It is also essential for the analyst to look at similar policies and instruments that have been implemented in other governments to determine possible outcomes.

Step 3: Policy Network and Communication

Once the policy instrument has been decided, the next step is about assigning the new policy roles and developing a policy network. A policy network is about identifying all actors who will have a role in the implementation and have a stake in the new policy. This stage is not about assigning responsibilities and tasks but instead identifying actors who will play a part in this policy. Identifying the actors involved will help the analyst design a strategy that will assist in the next step of the implementation process. This stage is also about communicating the policy and why the problem the policy is trying to solve needs to be solved. An analyst at this stage must be transparent and have clear and concise facts about the policy and the problem. Again, correctly defining the problem plays a significant role. The issue at this stage is not communicating the policy vividly, which may cause the policy to not be supported. It is also important to remember that most public policies will have actors in different governments who will play a role in the policy. A way to address this problem is to develop a policy argument and agenda-setting.

Step 4: Implementation

At this stage, the policy analyst has now defined the problem completely, chosen the instrument to solve the problem, analyzed all alternatives for other instruments, and has developed a policy network. It is now time to implement the policy. Implementation of the policy is about assigning objectives to all of the roles identified in the policy network. The key to implementation is ensuring that all positions involved have an understanding of how the policy is going to be implemented. Peters (2016) points out three criteria needed for policy implementation, adequate time to implement, specific objectives, and agreed upon tasks for each role. Essentially the policy analyst must develop a clear and concise implementation strategy that is understood and agreed by all parties involved. The lack of this strategy is where the issue occurs at this stage. The most used form of the implementation strategy is forward mapping. Forward mapping begins by stating the precise goal of the policy. As an example, "it is the intent of this policy to combat hunger within our community by providing food to local food banks." The process of forward mapping then assigns roles based on specificity.

Step 5: Evaluation

The final step of policy analysis is evaluating the implemented policy. At this stage, the policy analyst looks at all outcomes of the policy to determine success. In doing this, all inputs to the policy are compared to the outputs to develop performance measures. These measures give key performance indicators to how well the policy is performing. In the case of the ransomware prevention policy presented in this project, all inputs and outputs will be developed into a logic model to demonstrate the desired outcomes and performance measures.

Policy Solution

Having examined the challenges local governments face in preventing ransomware and private sector solutions, we can now apply public policy analysis to develop a policy that is achievable by many local agencies. In doing so, this project will take each step of the policy analysis process previously discussed and apply local government mechanisms to achieve this goal. The first step of this process is properly defining the problem of how ransomware affects local governments and how implementing prevention is problematic in many agencies. It is essential in this step to identify all relevant stakeholders and how this policy may affect them. We will then use this problem definition to design instruments to assist in the mitigation of ransomware and a communication plan to all stakeholders. Finally, the project will provide implementation and evaluation, including a logic model.

Problem Definition

On the surface, ransomware appears to be a straightforward problem. A hacker deploys a nasty bug that encrypts files or lockdowns access to a PC or network. However, as discussed, ransomware presents serious complications for local government agencies. These complications must be a part of our problem definition. First, ransomware has severe implications for local governments due to the possible services the attack could disrupt. Ransomware attacks in the private sector may disrupt their day-to-day operations for a financial services company, as an example, without having life-changing implications. However, this is hardly the case for local agencies. In many of these cases, local government agencies provide vital lifesaving services that range from law enforcement to emergency medical services. Ransomware shutting down these types of services has the potential to affect lives negatively.

Further, local agencies lack the resources to respond adequately to ransomware attacks. It takes longer for a local agency to respond than in the private sector. Finally, ransomware attacks against local government agencies have full implications for their financial position. Look no further than the City of Atlanta, who spent over $60 million in migrating their attack and still did not recover any of the data (Lohrmann, 2019).

Local governments face issues in ransomware prevention due to inadequate funding for cybersecurity, which leads to the inability to attract staff and improper education programs. By defining both the implications and challenges of ransomware, the public policy process provides us with stakeholders. Defining the stakeholders allows us to design instruments to solve the problem. Notice that the list below is more of a grouping of stakeholders based on their relationship to this problem. Additionally, it is common for these stakeholders to overlap:

Stakeholders

- Taxpayers within the government's jurisdiction
- Government employees who utilize the IT infrastructure
- Elected officials
- IT professional within the local government
- Taxpayers and constituents who depend on government services
- Property owners within the agencies' jurisdiction
- Business owners within the agencies' jurisdiction

Instrument Design

This project covered three fundamental reasons why local government agencies have experienced issues with ransomware - lack of budgetary control, acquiring cybersecurity talent, and educating employees. The policy solution will contain instruments to combat these issues. First, the lack of budgetary control feeds the other two issues. Acquiring cybersecurity talent and educating employees is a result of a lapse in funding. We cannot combat these issues until we address the lack of funding. Our first instrument in this policy will be to introduce a cybersecurity program based on a performance-based budget. This process will guarantee the funds needed in areas such as acquiring cybersecurity talent and educating employees.

Performance budgeting, as described by Bland (2014), is a budgeting process that measures the actual performance of the line item expenditure and bases the allocation amount on this performance. The performance-based budgeting method accomplishes this by analyzing the goals and objectives and inputs, outputs, and outcomes (Bland, 2014). If a program is budgeted at the line item level through a performance-based budgeting methodology, the money allocated must be used for its specific goals. A ransomware prevention policy with a performance-based budget would then have an allocation that could only be used for items such as acquiring cybersecurity talent and educating employees.

It should be noted that there are drawbacks to performance-based budgeting. Using this type of budgeting method guarantees that the program is under constant scrutiny. Under a performance-based budget, the inputs, as well as the outputs, are continually being analyzed. Meaning if the outcome of the program does not meet its goals, then the inputs, such as funding, could be cut. Further, performance-based budgeting is tedious and requires constant analysis, which is why many agencies only utilize this practice for specific programs rather than the entire budget (Bland, 2014). However, to acquire funds for a ransomware prevention policy, performance-based budgeting is a mechanism that guarantees that allocating money will be spent on this policy.

Allocating funds for the policy now allows us to introduce instruments for the actual prevention of ransomware. In terms of acquiring cybersecurity talent, many local agencies need to come to a harsh truth – they cannot afford full-time cybersecurity positions. Most of these agencies' revenue streams, as discussed, are simply too volatile to take on the long term costs of these positions. As a result, agencies have one option, outsourcing. Fortunately, local agencies have mechanisms to assist them in this process - public, private partnerships, and franchising.   To understand the context of how these mechanisms will work in this policy, we will need to use a hypothetical agency. In this regard, we will use a fictional city, City A, to illustrate the utilization of public-private partnerships and franchising. City A is experiencing the issues we have previously discussed, including an uneven revenue stream and dilemmas in implementing cybersecurity solutions.

Public-private partnerships are programs that allow both a government agency and a private company to share the cost of a program while both receiving benefits (Kamensky et al., 2012). A public, private partnership allows a public agency to contract with a private sector organization to provide a service or product to the agency. In return, the private sector organization receives some incentive to do business with the public agency. Incentives in this regard come in all shapes and sizes and range from sharing revenues with the agency to tax benefits. Our public-private partnership for the ransomware prevention policy will first outsource the needed requirements. The requirements, in this case, are classified into two categories, infrastructure, and personnel. We know from our private sector solutions that the backing up of data and frequent patching off all relevant systems are two crucial elements in ransomware prevention. Fortunately, we can classify these needs into service for the sake of our public-private partnership that captures each of these aspects. Our policy solution will mandate the contracting of data backups to an offsite cloud location and the patching of all relevant software by an outside company. In addition, this company will analyze the status of our network infrastructure, including firewalls, to determine their status and if a replacement is needed. This company will then provide all hardware and implement the hardware. Finally, our policy will mandate a minimum contract period of five years. This is a large project that will require a private sector company to be in the vicinity of City A. However, this directly relates to how we will incentivize a company to provide these services through franchising these services to other agencies. Franchising in the public sector is when one agency offers services to another local agency (Kamensky et al, 2012). We know that City A will have to pay for these services. However, we also know like many local agencies, City A cannot afford the total long-term costs. To combat this, City A will establish franchise contracts with other local agencies for the private sector company to provide the same services. Other local agencies, as we know, are facing the same issues in combating ransomware. In the case of our ransomware prevention policy, this franchising mechanism will spread the cost to several agencies instead of one, thereby lowering the overall cost.

Data backup and patching of operating systems is only one part of the private sector solution. The other part, as we know, relates to the cybersecurity education of employees. For this solution, we will also rely on public-private partnerships, but instead of collaborating with a private company, we will look at another valuable resource, higher education. Cybersecurity is becoming a very popular major. In 2018, cybersecurity was the most prevalent degree colleges added to their majors (Busta, 2018). Local agencies should address this in their ransomware solutions. The NAISCO survey (2018) listed partnerships with higher education as a fundamental solution for local agencies' cybersecurity needs. For our ransomware prevention policy, City A will collaborate with surrounding universities offering cybersecurity as a major to develop training for employees. The incentive in this case for the university is the real-world experience it can offer its students.

The other issue with education, as we know, deals with incentivizing employees to learn the material in a cybersecurity class. To combat this issue, we can implement a strategy that has proven successful in a few agencies. This strategy has only been implemented on a small scale.   A small number of agencies now require employees to take cybersecurity training and pass a test, and when they do so, they are offered paid time off (PTO) for passing the test (Parnofiello, 2019). This incentive of paid time off is a simple solution public agencies can implement at a low cost to help ensure employees are learning the material.

Policy Communication

With our instruments defined, we can now begin to communicate the policy to appropriate stakeholders. This policy will require approval from City A's elected body for our public-private partnerships and their corresponding contracts. This approval includes the addition of our performance-based budget to the City’s overall budget, which will guarantee funding and the City's permission to solicit for the partnerships. In this case, we will solicit using a request for proposal (RFP), which obligates our contracted private-sector provider as well as our education partner to standard contract language. Once adopted by the elected body, a policy manager will be assigned. This manager will be tasked with identifying all relevant actors and communicating the policy to them. It is important to note that policy communication is frequently ongoing throughout the life of the policy, and the policy manager will reach out to all prospective agencies regarding our franchising instrument.

Policy Implementation

For the implementation of our policy, the policy manager will enact a forward mapping process. In this case, we must identify the overall goal of our policy and the inputs through our instruments that will achieve this goal. The overall goal of this policy, as we know, is ransomware prevention. Additionally, we know the inputs from our instrument design. Note that the inputs are not just the instruments themselves but also the mechanisms we need to implement and support those instruments:

- Partnerships with a private firm to provide cybersecurity support
- Partnership with an educational institution for educational support
- Request for proposals (RFP's)
- Management of Public-Private Partnerships
- Policy Manager
- Performance-Based Budget
- Paid Time Off Programs
- Education Platforms for Cybersecurity Training

With our inputs defined, the policy manager can now implement the policy through the establishment of steps:

1. Develop a Performance-Based Budget with Performance Measures
2. Submit Performance-Based Budget for Approval
3. Develop RFP's
4. Award RFP's and Finalize Contracts
5. Contracted Private Sector Vendor Provides Cybersecurity Support
6. Contracted Educational Institution Provides Education Platforms
7. Develop Franchise Contracts with Other Agencies
8. Testing of Employees for Cybersecurity Awareness

These steps are high-level, and there are many sub-steps for each of the top-level steps. However, these steps and inputs layout an overall map of how to implement such a policy. Further, the inputs and steps provide a foundation for the final stage of our policy solution – evaluation.

Policy evaluation

The evaluation of this policy will involve establishing performance measures and comparing all inputs and outputs to desired outcomes. We will select three performance measures for ransomware prevention policy:

1. 60% of all employees achieve a passing score on their cybersecurity training exam
2. Data backups will occur every 24 hour
3. All software will be patched within one week of manufacture, releasing the patch.

Performance measure 1 and 2 will require the establishment of the data that requires backing up, and what software is deemed crucial to require patching. The policy will require the development of a logic model to evaluate the outcomes of the policy's performance with the required inputs. This logic model will provide a success rate by comparing the outcomes of the logic model with our established performance measures. Frechtling (2007) defines a logic model as a tool that is utilized to describe the change and impact of a project or policy. In the case of our ransomware prevention policy, a logic model compares all of the required inputs, the activities of those inputs, the outputs of those activities, and the overall outcomes to determine the policy's success. A logic model sample of our ransomware prevention policy is provided in Appendix (A).

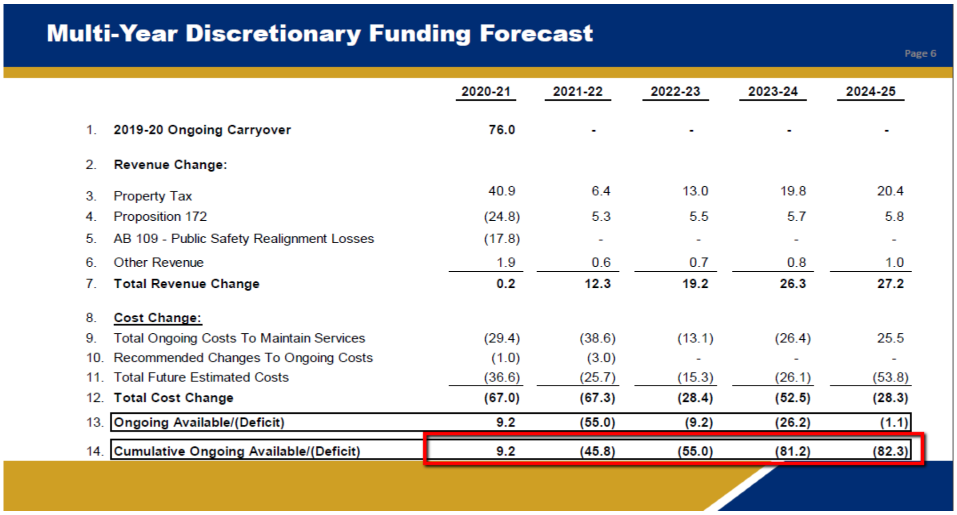
CHAPTER FIVE
CASE STUDY - COUNTY OF SAN BERNARDINO

We have developed a hypothetical policy to combat ransomware within local government agencies by analyzing private sector solutions and the public policy process. This theoretical policy utilized tools such as public-private partnerships and performance-based budgeting to implement measures in ransomware prevention, including software patching and educational programs to employees. This project will now examine how a real, local government agency is implementing solutions to combat ransomware and the challenges the agency is facing in implementing these solutions. These solutions and challenges will directly relate to the solution and challenges previously presented in this project. This project will focus on the problem questions given at the beginning of this project:

- What are the challenges for implementing such best practices in local governments within the United States?
- What are the specific practical solutions available to help local governments combat ransomware attacks?
- What resources can local governments utilize from other aspects of government operations to assist in developing a ransomware prevention policy?

For our real-world agency, this project will examine the County of San Bernardino, who shares similarities to our hypothetical city utilized in our policy solution. The County of San Bernardino is the largest geographical agency in the agency in the United States. As a result, this county government provides an array of services to a very diverse population and must provide these services to geographical locations that vary from deserts to mountains. The County of San Bernardino currently employees over 22,000 employees, and most employees have network and internet access to accomplish their everyday tasks. The County of San Bernardino has had a curious financial history, including a severe budget gap of $46 million in 2011 and submitting balanced budgets for the last three fiscal years (CAP Review, 2019). Of particular interest is the fact that the County of San Bernardino has not fallen prey to a ransomware attack. However, this does not mean that ransomware attacks have not occurred within San Bernardino County. In October of 2019, hackers infected the San Bernardino City Unified School District with ransomware that resulted in the loss of internal employee email capabilities (De Atley, 2019). In 2018, the County launched a cybersecurity division within its Information Services Department and hired a chief security officer to oversee the division. While the County has implemented measures to combat ransomware and other cybersecurity issues, they also face challenges in tackling these issues, each of which is discussed in our case study. What are the challenges San Bernardino County is facing in implementing such best practices?

The County of San Bernardino is currently experiencing a fundamental issue implementing a full-scale cybersecurity policy that fulfills all of the best practices from our private sector solutions. We know from our previous analysis, budgetary problems are the catalyst for other problems in implementing cybersecurity solutions within local government agencies. Of particular concern is a volatile revenue that results in inconsistency in an agency's revenue stream. The County of San Bernardino is not immune to this issue. First, let us examine the County's projected financial position over the next five fiscal years. Chief Executive Officer Gary McBride presented the image below from a financial position presentation to County Board of Supervisors on May 5, 2020:



Multi-Year Discretionary Funding Forecast

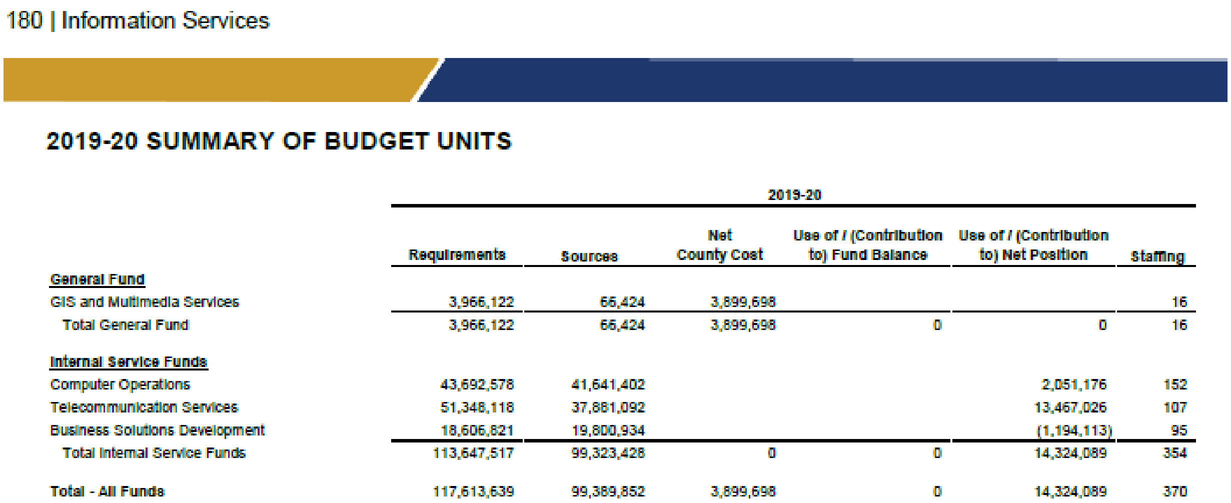
Page 6

		2020-21	2021-22	2022-23	2023-24	2024-25
1.	**2019-20 Ongoing Carryover**	**76.0**	**-**	**-**	**-**	**-**
2.	**Revenue Change:**					
3.	Property Tax	40.9	6.4	13.0	19.8	20.4
4.	Proposition 172	(24.8)	5.3	5.5	5.7	5.8
5.	AB 109 - Public Safety Realignment Losses	(17.8)	-	-	-	-
6.	Other Revenue	1.9	0.6	0.7	0.8	1.0
7.	**Total Revenue Change**	**0.2**	**12.3**	**19.2**	**26.3**	**27.2**
8.	**Cost Change:**					
9.	Total Ongoing Costs To Maintain Services	(29.4)	(38.6)	(13.1)	(26.4)	25.5
10.	Recommended Changes To Ongoing Costs	(1.0)	(3.0)	-	-	-
11.	Total Future Estimated Costs	(36.6)	(25.7)	(15.3)	(26.1)	(53.8)
12.	**Total Cost Change**	**(67.0)**	**(67.3)**	**(28.4)**	**(52.5)**	**(28.3)**
13.	**Ongoing Available/(Deficit)**	**9.2**	**(55.0)**	**(9.2)**	**(26.2)**	**(1.1)**
14.	**Cumulative Ongoing Available/(Deficit)**	**9.2**	**(45.8)**	**(55.0)**	**(81.2)**	**(82.3)**

Figure 2. County of San Bernardino Projected 5 Year Budget
http://cms.sbcounty.gov/cao-finance/Budget.aspx

Notice that there is a five-year budget deficit of $82.3 million as projected by the

County Administrative Office. This deficit is primarily due to an expected decline in revenue. This deficit additionally means that the County of San Bernardino will face challenges in obligated long-term funds for full-time positions to combat ransomware and other cybersecurity measures. This issue, as we know, is a prevalent problem among local government agencies. The County also faces problems in allocated funds that are committed to cybersecurity. While the County has implemented a cybersecurity program, at a budgetary level, they do not have specific line items allocated to cybersecurity expenses. The image below was taken from the County of San Bernardino 2019-2020 adopted budget:



180 | Information Services

2019-20 SUMMARY OF BUDGET UNITS

	2019-20					
	Requirements	Sources	Net County Cost	Use of / (Contribution to) Fund Balance	Use of / (Contribution to) Net Position	Staffing
General Fund						
GIS and Multimedia Services	3,966,122	66,424	3,899,698			16
Total General Fund	3,966,122	66,424	3,899,698	0	0	16
Internal Service Funds						
Computer Operations	43,692,578	41,641,402			2,051,176	152
Telecommunication Services	51,348,118	37,881,092			13,467,026	107
Business Solutions Development	18,606,821	19,800,934			(1,194,113)	95
Total Internal Service Funds	113,647,517	99,323,428	0	0	14,324,089	354
Total - All Funds	117,613,639	99,389,852	3,899,698	0	14,324,089	370

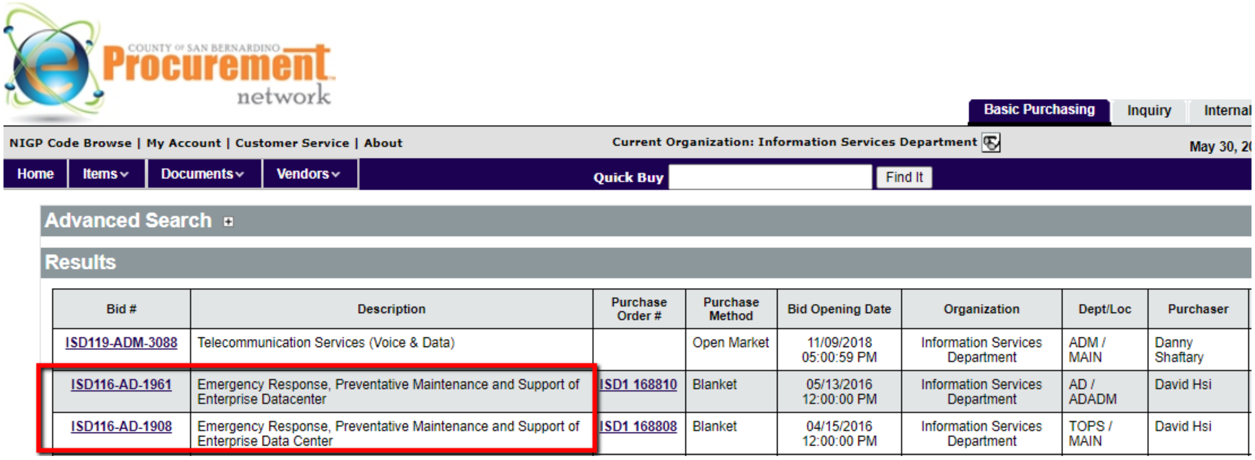
Figure 3. County of San Bernardino 2019-2020 Adopted Budget
http://cms.sbcounty.gov/cao-finance/Budget.aspx

Of particular interest is the Information Services Department does not have a budgetary unit dedicated to information assurance or cybersecurity. Instead, these operations are lumped together with other department initiatives. As previously discussed, this often results in competition between department objectives and can lead to the underfunding of specific actions, like cybersecurity.

Recommended Action: The County of San Bernardino should implement a performance-based budget for cybersecurity activities. This action will assist in ensuring direct funding for these initiatives. Additionally, given the number of cities within San Bernardino County, the County should explore franchising their cybersecurity services once established.

What resources can the County utilize from other aspects of their operations to assist in developing a ransomware prevention policy?

The County of San Bernardino, like many other local government agencies, faces issues in allocating direct funds for cybersecurity programs. Additionally, there are other aspects of private-sector solutions the County can utilize in combating ransomware. From the County's current budget position, we know that obligating the long term costs of cybersecurity is an issue and will continue to be so over the next five fiscal years. As previously discussed, a solution to this issue is to outsource cybersecurity services to an outside company. Of particular importance, is the routinely backing up of data to ensure data recovery in the case of ransomware. The County of San Bernardino is not currently utilizing this solution to outsource its data backup initiatives. However, this service was, in fact, outsourced previously to a private sector entity. An examination of the County's electronic procurement system reveals that the County contracted for this service in 2015:

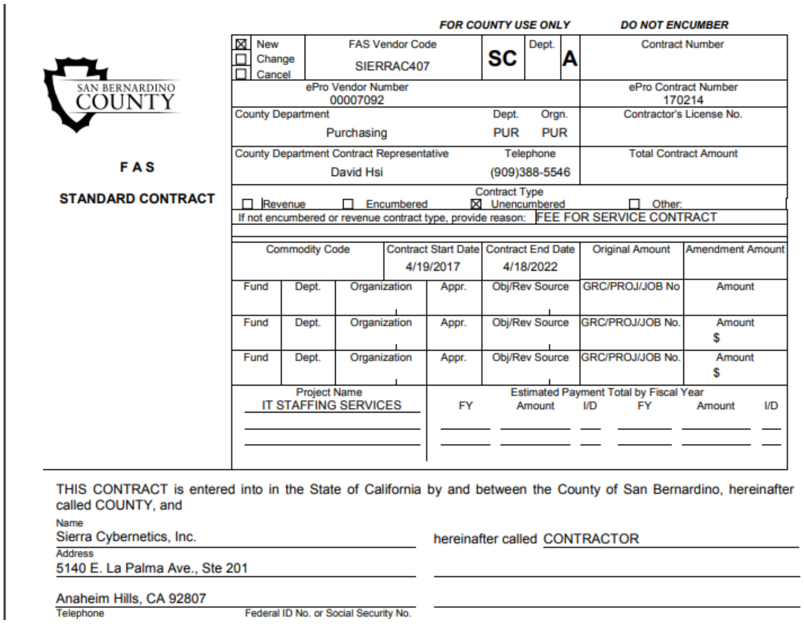


Bid #	Description	Purchase Order #	Purchase Method	Bid Opening Date	Organization	Dept/Loc	Purchaser
ISD119-ADM-3088	Telecommunication Services (Voice & Data)		Open Market	11/09/2018 05:00:59 PM	Information Services Department	ADM / MAIN	Danny Shaftary
ISD116-AD-1961	Emergency Response, Preventative Maintenance and Support of Enterprise Datacenter	ISD1 168810	Blanket	05/13/2016 12:00:00 PM	Information Services Department	AD / ADADM	David Hsi
ISD116-AD-1908	Emergency Response, Preventative Maintenance and Support of Enterprise Data Center	ISD1 168808	Blanket	04/15/2016 12:00:00 PM	Information Services Department	TOPS / MAIN	David Hsi

Figure 4. Related Solicitations (RFP's) to Information Assurance and Cybersecurity https://epro.sbcounty.gov/bso/

It is important to note that the County bid out these contracts in 2016 with a three-year contract period, meaning that the County does not have a current contract. It is assumed that these services are now provided "in-house," which could mean that the County is not fully utilizing data backups to the best of their abilities. In this regard, the County is maybe falling short of best practice used in the private sector. However, this is not to say the County has not implemented measures in outsourcing their cybersecurity needs. In 2017, the County did execute a contract for outsourcing some of their IT reeled needs, including

Business Systems Analysts who could assist in information assurance and cybersecurity needs.



SAN BERNARDINO COUNTY

F A S

STANDARD CONTRACT

FOR COUNTY USE ONLY   DO NOT ENCUMBER

☒ New □ Change □ Cancel	FAS Vendor Code SIERRAC407	SC	Dept. A	Contract Number
ePro Vendor Number 00007092				ePro Contract Number 170214
County Department Purchasing	Dept. PUR	Orgn. PUR		Contractor's License No.
County Department Contract Representative David Hsi	Telephone (909)388-5546			Total Contract Amount

Contract Type
□ Revenue   □ Encumbered   ☒ Unencumbered   □ Other:
If not encumbered or revenue contract type, provide reason: FEE FOR SERVICE CONTRACT

Commodity Code	Contract Start Date	Contract End Date	Original Amount	Amendment Amount
	4/19/2017	4/18/2022		

Fund	Dept.	Organization	Appr.	Obj/Rev Source	GRC/PROJ/JOB No	Amount
Fund	Dept.	Organization	Appr.	Obj/Rev Source	GRC/PROJ/JOB No.	Amount $
Fund	Dept.	Organization	Appr.	Obj/Rev Source	GRC/PROJ/JOB No.	Amount $

Project Name
IT STAFFING SERVICES

Estimated Payment Total by Fiscal Year
FY   Amount   I/D   FY   Amount   I/D

THIS CONTRACT is entered into in the State of California by and between the County of San Bernardino, hereinafter called COUNTY, and

Name
Sierra Cybernetics, Inc.   hereinafter called CONTRACTOR

Address
5140 E. La Palma Ave., Ste 201

Anaheim Hills, CA 92807

Telephone   Federal ID No. or Social Security No.

Figure 5. Current IT Staffing Contract https://epro.sbcounty.gov/bso/

Recommended Action: Given the County's current financial position, which does not account for the current COVID19 pandemic expenses, the County should utilize additional outsourcing mechanisms to reduce costs, as suggested in this project’s policy solution.

What are the practical solutions available to help the County of San Bernardino combat ransomware attacks?

As previously mentioned, the County initiated an information security strategic plan in 2018. Their information security plan is fundamental in establishing a baseline to secure cybersecurity-related activities within the County. Further, this plan included measures to increase information assurance, such as identifying and classifying data, enabling data backup protocols, establishing risk assessments, and implementing monitoring tools. Below, is a roadmap of the County's information security plan:

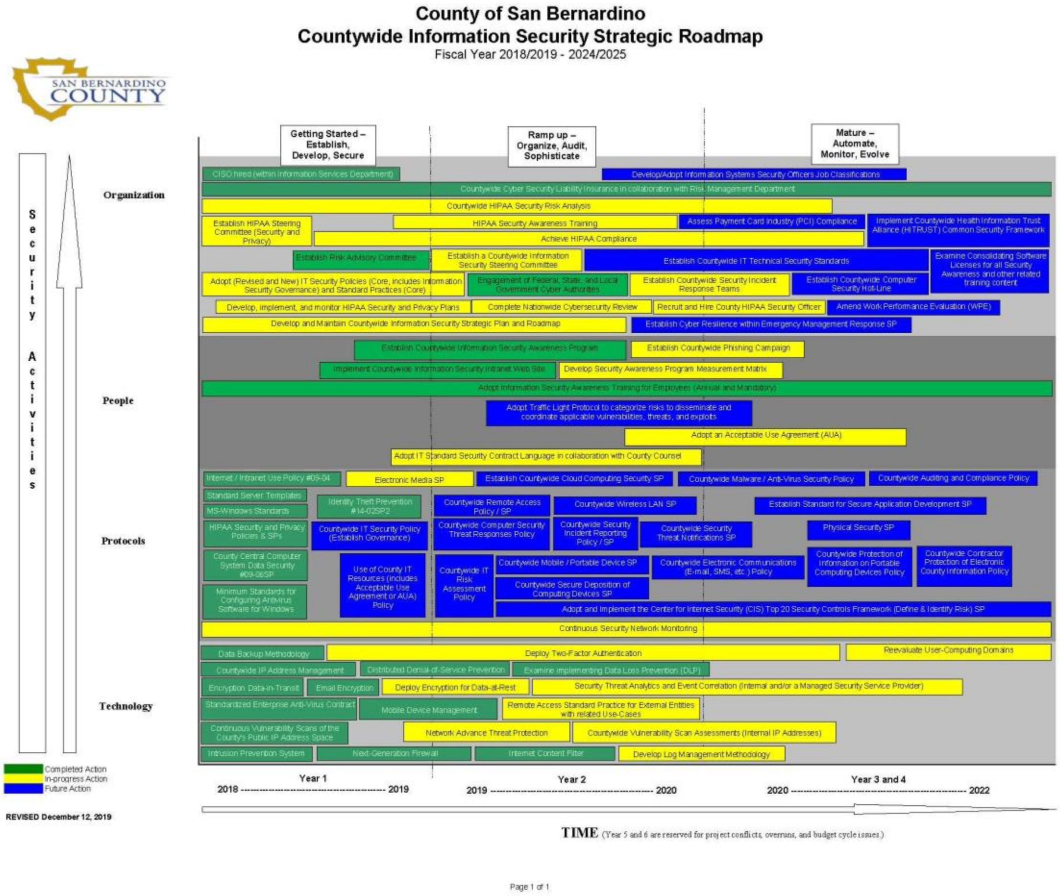

County of San Bernardino
Countywide Information Security Strategic Roadmap
Fiscal Year 2018/2019 - 2024/2025
SAN BERNARDINO COUNTY
Getting Started – Establish, Develop, Secure
Ramp up – Organize, Audit, Sophisticate
Mature – Automate, Monitor, Evolve
Security Activities
Organization
CISO hired (within Information Services Department)
Develop/Adopt Information Systems Security Officers Job Classifications
Countywide Cyber Security Liability Insurance in collaboration with Risk Management Department
Countywide HIPAA Security Risk Analysis
Establish HIPAA Steering Committee (Security and Privacy)
HIPAA Security Awareness Training
Assess Payment Card Industry (PCI) Compliance
Implement Countywide Health Information Trust Alliance (HITRUST) Common Security Framework
Achieve HIPAA Compliance
Establish Risk Advisory Committee
Establish a Countywide Information Security Steering Committee
Establish Countywide IT Technical Security Standards
Examine Consolidating Software Licenses for all Security Awareness and other related training content
Adopt (Revised and New) IT Security Policies (Core, includes Information Security Governance) and Standard Practices (Core)
Engagement of Federal, State, and Local Government Cyber Authorities
Establish Countywide Security Incident Response Teams
Establish Countywide Computer Security Hot-Line
Develop, implement, and monitor HIPAA Security and Privacy Plans
Complete Nationwide Cybersecurity Review
Recruit and Hire County HIPAA Security Officer
Amend Work Performance Evaluation (WPE)
Develop and Maintain Countywide Information Security Strategic Plan and Roadmap
Establish Cyber Resilience within Emergency Management Response SP
People
Establish Countywide Information Security Awareness Program
Establish Countywide Phishing Campaign
Implement Countywide Information Security Intranet Web Site
Develop Security Awareness Program Measurement Matrix
Adopt Information Security Awareness Training for Employees (Annual and Mandatory)
Adopt Traffic Light Protocol to categorize risks to disseminate and coordinate applicable vulnerabilities, threats, and exploits
Adopt an Acceptable Use Agreement (AUA)
Adopt IT Standard Security Contract Language in collaboration with County Counsel
Protocols
Internet / Intranet Use Policy #09-04
Electronic Media SP
Establish Countywide Cloud Computing Security SP
Countywide Malware / Anti-Virus Security Policy
Countywide Auditing and Compliance Policy
Standard Server Templates
MS-Windows Standards
Identity Theft Prevention #14-02SP2
Countywide Remote Access Policy / SP
Countywide Wireless LAN SP
Establish Standard for Secure Application Development SP
HIPAA Security and Privacy Policies & SPs
Countywide IT Security Policy (Establish Governance)
Countywide Computer Security Threat Responses Policy
Countywide Security Incident Reporting Policy / SP
Countywide Security Threat Notifications SP
Physical Security SP
County Central Computer System Data Security #09-06SP
Use of County IT Resources (includes Acceptable Use Agreement or AUA) Policy
Countywide IT Risk Assessment Policy
Countywide Mobile / Portable Device SP
Countywide Electronic Communications (E-mail, SMS, etc.) Policy
Countywide Protection of Information on Portable Computing Devices Policy
Countywide Contractor Protection of Electronic County Information Policy
Minimum Standards for Configuring Antivirus Software for Windows
Countywide Secure Deposition of Computing Devices SP
Adopt and Implement the Center for Internet Security (CIS) Top 20 Security Controls Framework (Define & Identify Risk) SP
Continuous Security Network Monitoring
Technology
Data Backup Methodology
Deploy Two-Factor Authentication
Reevaluate User-Computing Domains
Countywide IP Address Management
Distributed Denial-of-Service Prevention
Examine implementing Data Loss Prevention (DLP)
Encryption Data-in-Transit
Email Encryption
Deploy Encryption for Data-at-Rest
Security Threat Analytics and Event Correlation (Internal and/or a Managed Security Service Provider)
Standardized Enterprise Anti-Virus Contract
Mobile Device Management
Remote Access Standard Practice for External Entities with related Use-Cases
Continuous Vulnerability Scans of the County's Public IP Address Space
Network Advance Threat Protection
Countywide Vulnerability Scan Assessments (Internal IP Addresses)
Intrusion Prevention System
Next-Generation Firewall
Internet Content Filter
Develop Log Management Methodology
🟩 Completed Action
🟨 In-progress Action
🟦 Future Action
REVISED December 12, 2019
Year 1
2018 -- 2019
Year 2
2019 -- 2020
Year 3 and 4
2020 -- 2022
TIME (Year 5 and 6 are reserved for project conflicts, overruns, and budget cycle issues.)
Page 1 of 1

Figure 6. County of San Bernardino Information Security Roadmap
http://cms.sbcounty.gov/cao-finance/Budget.aspx

The County's information security plan and roadmap are comprehensive, including many of the solutions proposed in this project. However, what is important is how the County will implement many of these objectives. Our case study has revealed that the County is not currently outsourcing many of these activities, and the County will face a substantial budget deficit over the next five years. For the County to implement many of the objectives listed on their information security roadmap, they must overcome these issues. To do so, the County must adopt measures and procedures that will introduce policies that guarantee the implementation of ransomware prevention and cybersecurity as a whole.

Recommended Action: To see their information security plan come to fruition over the next five years, the County must utilize innovative measures as discussed in this project to ensure they are implemented. These include the adoption of a performance-based budget for cybersecurity-related activities and the use of the public, private partnerships.

Conclusion

This project proposed a question of why local government agencies face issues in preventing ransomware from a public policy perspective. This project explored the history and functionality of ransomware. In its earliest form, ransomware was a modest issue in terms of the damage it could impose. However, over the last several decades, ransomware has evolved and has given hackers the capabilities to fully lock down networks and prevent government agencies from accessing crucial data. Once locked down, the hacker can then hold the data for ransom and prevent local governments from providing services.

Due to the potential profits, ransomware has become a very prominent form of malware, particularly for local government agencies. As this project explored, these agencies face significant challenges in not only preventing ransomware, but also all areas of cybersecurity. These challenges begin with the mandated budgeting processes local government agencies utilize. These budgeting limitations lead to deficiencies in IT infrastructure, obtaining cyber security-based personnel, and employee education programs. Each of these elements provides solutions that prevent ransomware. Additionally, as suggested by this project, local government agencies should implement ransomware and other cybersecurity solutions that exist in the private sector.

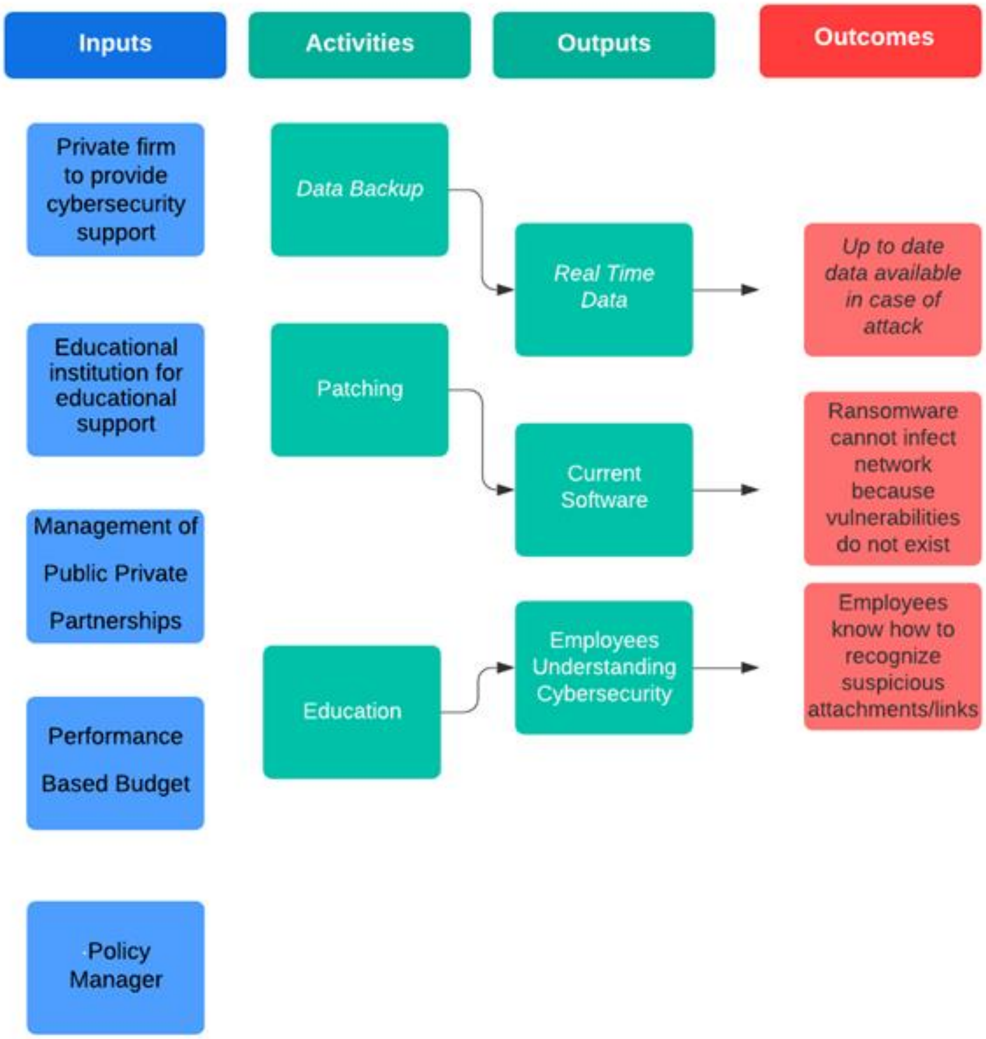
While ransomware solutions do exist and are successful in the private sector, local government agencies have failed to implement many of these solutions. The primary reason why these agencies have not been able to do so is their lack of implementing policies and mechanisms that guarantee ransomware prevention solutions come to fruition. This project analyzed the fundamental steps of the public policy process to provide requirements of how a local government agency could design such a policy. Further, the project provided a hypothetical policy that included solutions from the private sector and the tools local government agencies have at their disposal to implement such a policy.

Finally, a case of the County of San Bernardino demonstrated that while local government agencies have partially implemented private sector solutions, many are failing to implement a comprehensive policy-based solution. As stated previously, local governments must implement policies that are specific to ransomware. Failing to have these particular policies leads to a competition of resources, which results in resources being allocated elsewhere within the government agency. These policies must include funding and contacting mechanisms to provide the needed resources, which will secure policy success.

Ransomware in the future will evolve. Hackers will discover new vulnerabilities and will continue to target government agencies as well as private sector entities. Local government agencies have no choice but to develop a means to prevent these attacks. These agencies have a unique challenge in implementing such measures compared to their private-sector counterparts. A private company can buy and then implement a solution. In contrast, a government agency must follow statutes and policies to implement solutions and overcome the challenges discussed in this project. Ransomware prevention and cybersecurity must be policy-based as it promises long-term and committed solutions to these problems.

APPENDIX A

LOGIC MODEL


Inputs
Activities
Outputs
Outcomes
Private firm to provide cybersecurity support
Educational institution for educational support
Management of Public Private Partnerships
Performance Based Budget
Policy Manager
Data Backup
Patching
Education
Real Time Data
Current Software
Employees Understanding Cybersecurity
Up to date data available in case of attack
Ransomware cannot infect network because vulnerabilities do not exist
Employees know how to recognize suspicious attachments/links

APPENDIX B

NAISCO 2018 CYBERSECURITY SURVEY HIGHLIGHTS

Since 2010, CISOs have been challenged by insufficient funding and cyber talent availability

Identify the top barriers that your state faces in addressing cybersecurity challenges (top three per study).

	2010	2012	2014	2016	2018
1	Lack of sufficient funding	Lack of sufficient funding	Lack of sufficient funding	Lack of sufficient funding	Lack of sufficient cybersecurity budget
2	Increasing sophistication of threats	Increasing sophistication of threats	Increasing sophistication of threats	Inadequate availability of professionals	Inadequate cybersecurity staffing
3	Inadequate availability of security professionals	Inadequate availability of professionals	Inadequate availability of professionals	Increasing sophistication of threats and lack of documented processes	Increasing sophistication of threats

FIGURE 2

Current cyber FTE averages for states still fall below the average number of cyber FTEs employed by financial services institutions in 2010

How many dedicated cybersecurity professionals does your enterprise security office employ?

1–5
FTE average
2010 state cyber FTE professionals

>100
FTE average
2010 financial services* cyber FTE professionals

6–15
FTE average
2018 state cyber FTE professionals

FIGURE 3

Almost half of states do not have a separate budget line item for cybersecurity

Does your state have a cybersecurity budget line item? (50 respondents)

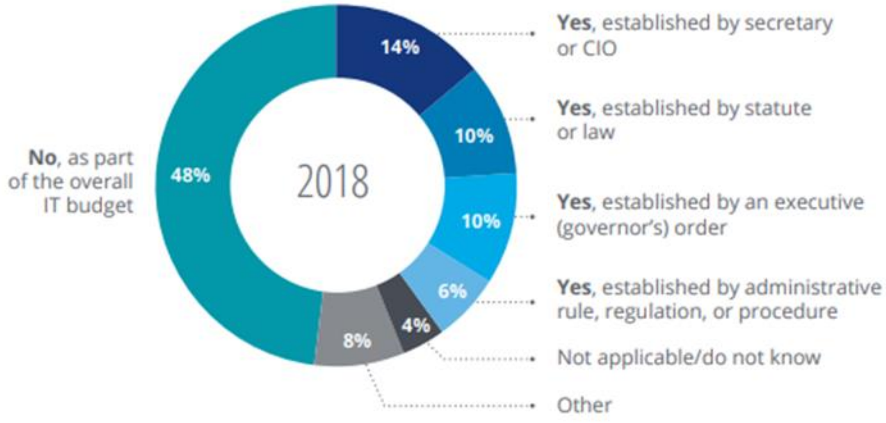


FIGURE 4

CISO budgets are growing slowly; compared to 2016, only an additional two states have reported a budget increase

Characterize the year-over-year trending in your state's cybersecurity budget for years 2016 and 2017. (49 respondents)

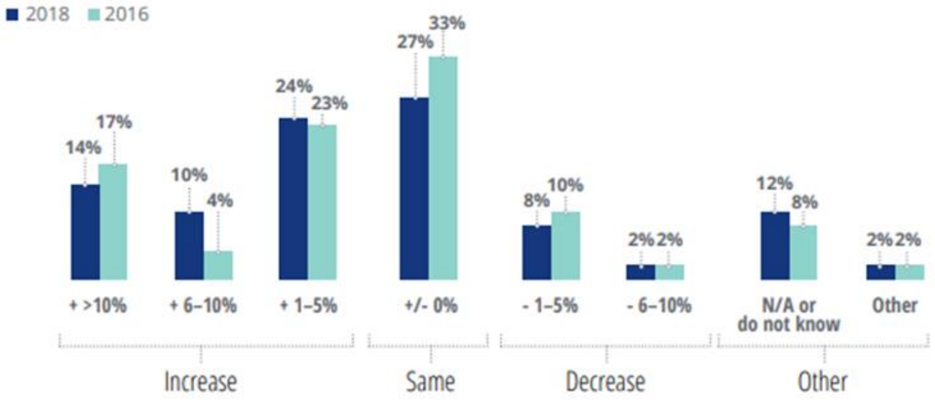
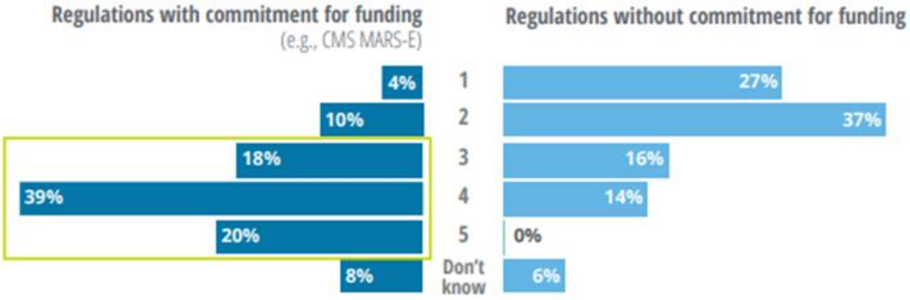


FIGURE 6

Cybersecurity initiatives can be more effective with committed funding

How effective are applicable federal and state cybersecurity regulations at improving your state's cybersecurity posture and reducing risk? (1 = least effective, 5 = most effective) (49 respondents)



While outsourcing has increased for certain functions, more than half of US states have yet to outsource many of them

Select the cybersecurity functions that your state outsources. (47 respondents)

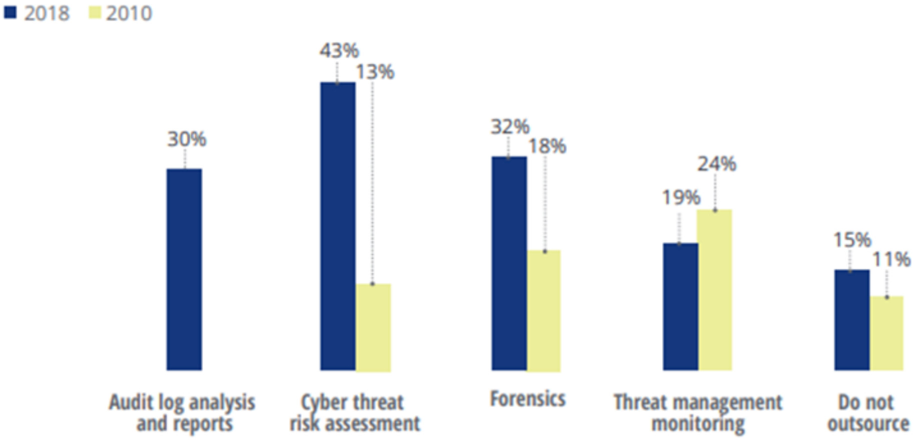
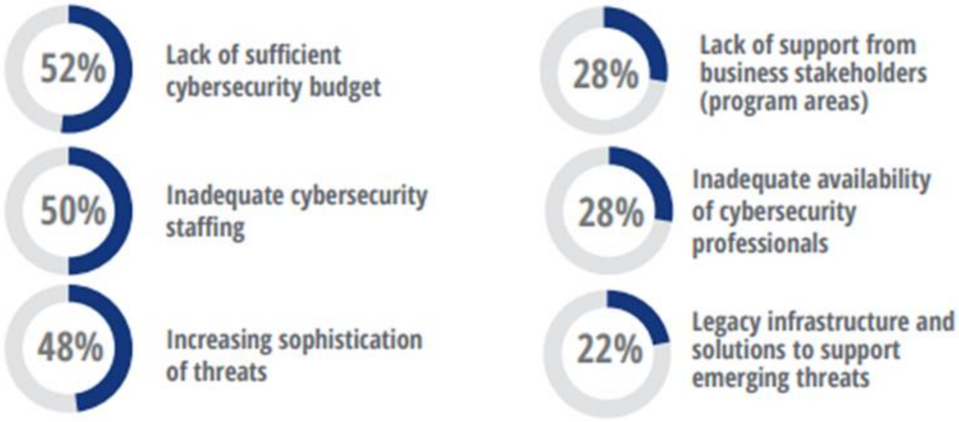


FIGURE 13

Budget and staffing remain top barriers to an effective cyber program

Identify the top five barriers that your state faces in addressing cybersecurity challenges. (50 respondents)



REFERENCES

Ahmed, M. R., Juremi, J., & Ramli, J. (2019). Ransomware: The evolution of a cybercrime. *International Journal of Psychosocial Rehabilitation*, 23(4), 1228–1237.

Bland, Robert (2014). *A budgeting guide for local government*. ICMA Press

Brandt, Andrew, Lowman, Mark (2020). Living off another land: Ransomware borrows vulnerable driver to remove security software. Sophos News. Retrieved April 11, 2020, from https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/

Busta, Hallie (2019). Colleges address cybersecurity training gap with degrees, partnerships. Education Dive. Retrieved on May 5, 2020, from https://www.educationdive.com/news/colleges-address-cybersecurity-training-gap-with-degrees-partnerships/533355/

CAP review of the 2019-20 San Bernardino County budget (March 2019). Retrieved May 11, 2020, from https://www.california-partnership.org/content/cap-review-2019-20-san-bernardino-county-budget

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success*.* *Journal of Homeland Security & Emergency Management*, 9(2), 1–22.

De Atley, Richard (2019). California school district's servers down after cyberattack*.* Govtech. Retrieved May 12, 2020, from https://www.govtech.com/security/California-School-Districts-Servers-Down-After-Cyberattack.html

Evangelakos, Gus (2019). Three ways to protect your city government from a ransomware attack. American City and County. Retrieved on April 2, 2020, from https://www.americancityandcounty.com/2019/09/11/three-ways-to-protect-your-city-government-from-a-ransomware-attack/

Frechtling, Joy (2007). *Logic models in program evaluation*. Jossey-Bass

Freed, Benjamin (2019). Report: Two-thirds of ransomware attacks in 2019 targeted state and local governments*.* Statescoop Retrieved on March 31, 2020, from https://statescoop.com/report-70-percent-of-ransomware-attacks-in-2019-hit-state-and-local-governments/

Heineman, Robert, Bluhm, William, Peterson, Steven, Kearny, Edward (2011). *The world of the policy analyst*. Chatham House Publishers

Hoffman, Karen (2018). True crime: SamSam ransomware I am*.* Retrieved April 9, 2020, from https://www.scmagazine.com/home/security-news/true-crime-samsam-ransomware-i-am/

Hoppe, Robert (2018) *Rules-of-thumb for problem-structuring policy design, Policy Design and Practice*, 1:1, 12-29, DOI: 10.1080/25741292.2018.1427419

Johnson, Ben (2016). An example of how ransomware works. Carbonblack. Retrieved April 5, 2020, from https://www.carbonblack.com/2016/09/19/how-ransomware-works/

Jones, Sam (2017). Timeline: How the WannaCry cyber-attack spread. Retrieved on April 9, 2020, from https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23

Kamensky, John & Morales, Albert (2013). *Competition, choice, and incentives in government programs*. Rowman and Littlefield

Lohrmann, Dan (2019). 2019: The year ransomware targeted state & local governments. Govtech. Retrieved on April 20, 2020, from https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html

NASCIO 2018 Cybersecurity Study (2018). NASCIO. Retrieved March 20, 2020, from https://www2.deloitte.com/content/dam/insights/us/articles/4751_2018-Deloitte-NASCIO-Cybersecurity-Study/DI_2018-Deloitte-NASCIO-Cybersecurity-Study.pdf

Norris, D. F., Mateczun, L., Joshi, A., Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of Homeland Security & Emergency Management*, 15(3), N.PAG.

Palmer, Danny (2019). 30 years of ransomware: How one bizarre attack laid the foundations for the malware taking over the world? ZDnet. Retrieved on April 2, 2020, from https://www.zdnet.com/article/30-years-of-ransomware-how-one-bizarre-attack-laid-the-foundations-for-the-malware-taking-over-the-world/

Parnofiello, Matt (2019). Don't wait for an attack to do statewide cybersecurity training. State Tech. Retrieved on May 5, 2020, from https://statetechmagazine.com/article/2019/11/dont-wait-attack-do-statewide-cybersecurity-training

Peters, Guy (2016). *American public policy: Promise and performance*. CQ Press

Richardson, Ronny & North, Max M (2017). Ransomware: Evolution, mitigation and prevention. *Faculty Publications*. 4276. https://digitalcommons.kennesaw.edu/facpubs/4276

Shah, Anwar (2013). *Local public financial management*. The World Bank

Sussman, Bruce (2019). Baltimore, $18 million later: This is why we didn't pay the ransom. Secure World Expo. Retrieved April 11, 2020, from https://www.secureworldexpo.com/industry-news/baltimore-ransomware-attack-2019

Zamora, Wendy (2019). 2019 State of malware report: Trojans and cryptominers dominate threat landscape. Malware Bytes. Retrieved March 18, 2020, from https://blog.malwarebytes.com/malwarebytes-news/ctnt-report/2019/01/2019-state-malware-report-trojans-cryptominers-dominate-threat-landscape/