Cybersecurity Threat and Vulnerability Characterization for the

Water and Wastewater Systems Sector

A Master Thesis

Submitted to the Faculty

of

American Public University

by

Rebekah M Brown

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Arts

May 2018

American Public University

Charles Town, WV

ABSTRACT OF THE THESIS

Cybersecurity Threat and Vulnerability Characterization for the

Water and Wastewater Systems Sectors

by

Rebekah Brown

American Public University System, April 1, 2018

Charles Town, West Virginia

Professor Joseph Direnzo, Thesis Professor

Cybersecurity threats present a growing concern to critical infrastructure operators; however it is not always clear which threats present the most risk or how they should be prioritized in the water and wastewater systems sector. Best practices often assume a baseline understanding of threats and vulnerabilities without many details on how to develop this understanding. This research addresses the gaps in current guidance and literature by developing threat and vulnerability characteristics for use in cybersecurity risk analysis in the water sector. The research analyzes threats based on case studies of cybersecurity incidents and identifies the intent, opportunity, and capabilities of attackers. Vulnerabilities are analyzed based on reports of flaws in water sector technologies that attackers could leverage, identifying the level of criticality in the systems, the difficulty of leveraging the vulnerability, and where it can be exploited from. The findings revealed a pattern of moderately sophisticated adversaries exploiting vulnerabilities in web-based systems with access to control systems, along with several outlier threats that should also be considered in risk analysis. The new threat and vulnerability characteristics can be used with existing risk assessment frameworks such as RAMCAP framework used in the water sector or the NIST Cybersecurity Framework.

TABLE OF CONTENTS

CHAPTER

1. INTRODUCTION………………………………………………………...………..…8
2. LITERATURE REVIEW……………………………………………………………10

Water Security Post 9/11………………………….....………………………..…11

Risk Analysis Frameworks………………………………………………………13

Focusing on Cybersecurity………………….………………………………..….15

Operational Security Needs in the Water Sector……………………………..….18

Preparing for Destructive Cyber Attacks……………………..…………….……20

1. THEORETICAL FRAMEWORK…………………………………………….……..22
2. METHODOLOGY……………………………………………………………….….26
3. RESULTS……………………..………………………………………………….…28

Water Systems Sector Operations……………………………………………….29

Water Systems Sector Technologies………………………………………….....33

Threat Assessment…………………………………………………………...…..35

Vulnerability Assessment………………………………………………………..42

1. DISCUSSION………………………..………………………………………………46

Using Threat Characteristics in Risk Analysis………………………….…….…46

Using Vulnerability Characteristics in Risk Analysis…………………….……..47

Updating and Maintaining Characteristics…………………………………..…..48

LIST OF REFERENCES……………………………………………………….……….49

LIST OF FIGURES

FIGURE PAGE

1. The RAMCAP Process……………………………………………………......................13
2. Graphical Representation of an Attack Model………..…….…....………………………17
3. Systems Within the Water Sector…..……………………………………………………29

LIST OF TABLES

TABLE PAGE

1. Description of framework implementation tiers for cybersecurity risk…………….……15
2. Matrix of threat aspects from water sector case studies…………………………………39
3. Threat Characteristics – Process Sabotage………………………………………………42
4. Threat Characteristics – Theft or Diversion…………..…………………………………42
5. Vulnerability Characteristics………………………………….…………………………45

**Introduction**

“It has long been recognized that among public utilities, water supply facilities offer a particular vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace.”

* J. Edgar Hoover, Director of the Federal Bureau of Investigation, 1941

Water is a critical element of life; there are many things in modern life that people can do without, but water is not one of them. Most people in developed countries are accustomed to having water readily available and use it almost without a second thought. It is not necessary to think about how water gets to most homes or businesses unless something goes wrong: a pipe freezes or breaks, or containments are discovered due to infrastructure or oversight failures*.* The same aspects that make the water system so easy to take for granted also make it an appealing target for those who want to cause harm.

Having reliable infrastructure that citizens can count on to provide services in an expected, standardized and safe way - including transportation, energy, and water - are essential to any nation’s economic and civic well-being. The same aspects that make these systems critical to a functioning society also make them appealing targets to attackers seeking to cause disruption. The potential for threats against these systems are known. In 2003, the White House published the Homeland Security Presidential Directive 7 (HSPD 7) and created federal policy for identifying and prioritizing critical infrastructure to protect from terrorist attacks, defining critical infrastructure as the sectors that provide essential services that underpin American society. (The White House, 2003).

One of the sectors that was identified is the water and wastewater systems sector, which is made up of public drinking water systems and wastewater treatment systems. The Department of Homeland Security identified that attacks against this sector could result in a large number of illnesses or casualties, and would impact public health and economic stability (DHS, 2017).

In the fall of 2011, an undisclosed municipal water plant in Illinois noticed strange activity with the water pumps responsible for transporting water from the facility to customers. A few months later, one of the pumps began to power on and off in quick succession, and the pump burned out, impacting water distribution (Nakashima, 2011). The attack was tied to hackers in Russia who gained remote access to the plant, and was the very first instance of a destructive cyber-attack against critical infrastructure in the United States. Many years have passed since that first destructive attack, and the situation has only become more critical. Cybersecurity threats, defined as adversaries with the intent, capability, and opportunity to cause harm by targeting networks or networked technologies, are in the news nearly every day. Vulnerabilities, or flaws in computer systems that can be used by an adversary maliciously, are discovered in critical computer systems just as often. Knowing what threats and vulnerabilities to address is a difficult task, and misidentification or incorrect prioritization could have disastrous effects.

Seven years after the incident at the water utility in Illinois, which was the first documented destructive attack in the water sector, there remains a disconnect between those designing technologies and operating systems in the water and wastewater systems sector and those providing security recommendations. Much of the current cybersecurity guidance focuses on generalized threats to computers; very little research or guidance has been published on threats specific to the unique and complex technologies and processes in the water sector. Without knowing how cybersecurity threats will impact these technologies, it is difficult to know how to protect against them.

This research will identify which cybersecurity threats pose the greatest risk to the stability and security of technologies in the water and wastewater systems sector, and how those threats can be addressed by synthesizing information on water sector operations and cybersecurity threats. Cybersecurity threats are defined as the intent, capability, and opportunity to carry out an attack using cyber means. Risk is calculated by identifying the threat of, vulnerability to, and impact of a cybersecurity threat. There are several frameworks or standards that have been developed to help water sector owners and operators address cybersecurity risk, including guidance from the American Water Works Association (AWWA) and the National Institute of Standards and Technology (NIST) however these standards do not provide guidance on how to identify cybersecurity threats and vulnerabilities, and this research aims to address that gap. Once the most significant threats have been identified and prioritized based on the risks they present, specific recommendations for the implementation of security measures and processes to counter those threats can be made by following the guidance provided by AWWA and NIST. Existing literature can be used to begin to build a picture of why the identification of cybersecurity threats is so critical.

**Literature Review**

A review of the existing literature on cybersecurity threats in the water and wastewater systems sector paints a picture of a sector that understands the criticality of protection from these threat, and is striving to identify the best way to gain a better understanding of the problem and potential solutions. Previous cybersecurity incidents are analyzed to gain a better understanding of threats that have manifested (Abrams and Weiss, 2008; Rao and Francis, 2015; Dakin, Newman, and Groves, 2009; Horta, 2007; Taormina et al, 2017). Simulated attacks on modeled systems show potential or theoretical threats (Taormina, et al, 2017). Examples of non-cyber related incidents are used to show what the impact of an attack could be (Mathews, 2008; Morley 2009). The findings in much of the existing literature show that cybersecurity needs to be a factor in decision making in water utilities, and that the concept of a threat needs to be expanded to include more than physical or terrorism-related threats that had been the focus for the past two decades.

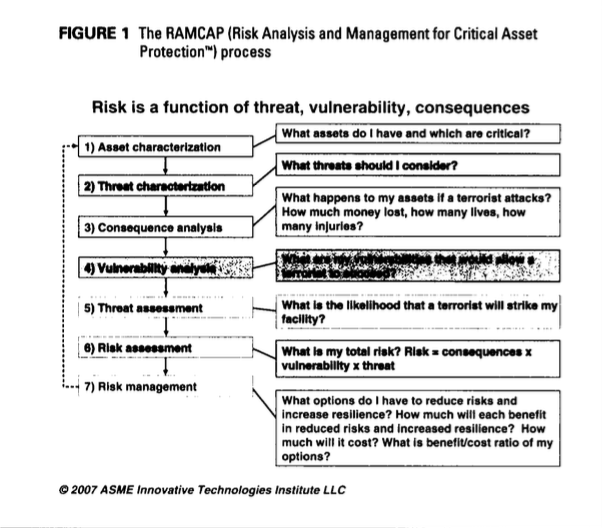
**Water Security Post 9/11**

Water security – the protection of critical water resources necessary to support life and the economy, has long been a focus of the industry. The concept of water security dates back as far as the 1600s where the plague was linked to contamination of the water supply (Sedlak, 2014) and as recent as the critical water shortage impacting Cape Town, South Africa (Muller, 2017). The terrorist attacks on September 11th prompted a new push for research into the threats facing critical infrastructure, including the water systems sectors (Kamien, 2006; Santora and Wilson, 2007). Stanely States, the Director of water quality for Pittsburg water and sewer authority and an expert on disaster recovery and resilience wrote that, “Prior to the attacks of September 11th, most emergency planning at utilities focused on accidents, equipment failures, and the specific natural disasters that are most likely to occur in a given water system’s location” (Kamien, 2006, pg 462). States went on to write that after September 11th, the focus of utilities shifted to incidents initiated by humans. Human-initiated attacks were included in emergency planning and disaster recovery documentation, however gaps in understanding were identified early on (Kamien, 2006, 2012; Santora and Wilson, 2007). The literature that was produced immediately following the terrorist attacks identified that there was still a lot of work that needed to be done to address the new threats. The Regional Disaster Resilience Guide identified that to ensure disaster preparedness for the water and wastewater sectors, there needed to be an improved understanding of the potential threats to the systems and their impact, enhanced ability to monitor systems for malicious activity, and increased access to information on threats (Kamien, 2006). Another critical step towards properly addressing threats is an improvement in the planning process, starting with the need of decision makers to allocate time toward identifying and mitigating risks (Santora and Wilson, 2007; Willis, et al, 2016).

Despite the emphasis on counter terrorism post-September 11th, a debate remains about whether there were significant threats to the water sector from human initiated activities (Lewis, 2002). John Lewis, representing the Center for Strategic and International Studies, disagreed with the focus on the threat of cyber terrorism, citing the fact that there has never been a successful terrorist attack on critical infrastructure. In the years since 2002 there have been multiple cyber attacks against critical infrastructure that impacted operations **(**Rao and Francis,2015; Horta, 2007**)**. There have been several reports of attempted or planned attacks against the water sector, including a 2002 arrest of a member of Al Qaeda with plans to target the U.S. Embassy in Rome by dumping cyanide into its water supply (Kroll, 2012).Fortunately for the water sectors, there have been several entities working to coordinate and standardize actions across the industry. These organizations include the Water Environment Federation (WEF), the Water Environment Research Foundation (WERF), and the American Water Works Association AWWA).

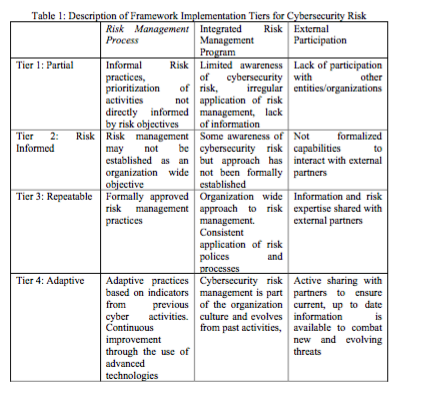
**Risk Analysis Frameworks**

The American Water Work Association was founded in 1881 as a body to foster, “…the exchange of information pertaining to the management of waterworks…and for securing economy and uniformity in the operations of waterworks” and is cited by the majority of literature on water security (Morely, 2010; Rao and Francis, 2015; Taoramina, et al.,2017; Santora and Wilson, 2007). AWWA has been critical in advocating the need for security in water sectors to meet the changing security needs. AWWA supported the implementation of the RAMCAP process, risk analysis management for critical asset management (Santora and Wilson, 2007; Morely, 2010).



The RAMCAP framework focused on the characterization of threats, vulnerabilities, and consequences of actions in the water sector, along with identifying built-in resilience and add-on security measures that could be used to mitigate identified risks. One champion of the RAMCAP method in the water sector is Kevin Morely, PhD, who has held many roles within the AWWA, including the Federal Manager. Dr. Morely has contributed a great to deal to the body of literature on water security and resilience in both the water distribution and wastewater treatment sectors. Morely wrote many of the papers published via AWWA regarding early water security, including the water/wastewater agency response network (WARN), which provides information and assistance to utilities in the case of an emergency (Morely, 2010). With the support of the AWWA, along with the Department of Homeland Security (DHS), the water sector began to focus more on water security, and specifically cybersecurity needs.

Another standard developed to assist with cybersecurity risk analysis is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2014; Shen, 2014). The NIST Cybersecurity Framework was developed following Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and was the government’s response to the problem of critical infrastructure owners and operators not knowing where to focus their attentions (Shen, 2014). The framework includes three parts, 1) the framework core, which includes cybersecurity guidance and best practices, 2) profiles, which help an organization understand the current and ideal state of their security programs, and 3) tiers, which can be used to self-identify where an organization sits from a program management perspective (NIST, 2014; Shen, 2014). Rao and Francis identified the tiers as a maturity model, and it is recommended by the AWWA to assess the maturity of cybersecurity practices in the water sectors (Rao and Francis, 2015). An example of the tiers, or maturity model, taken from the NIST Cybersecurity Framework is shown below.

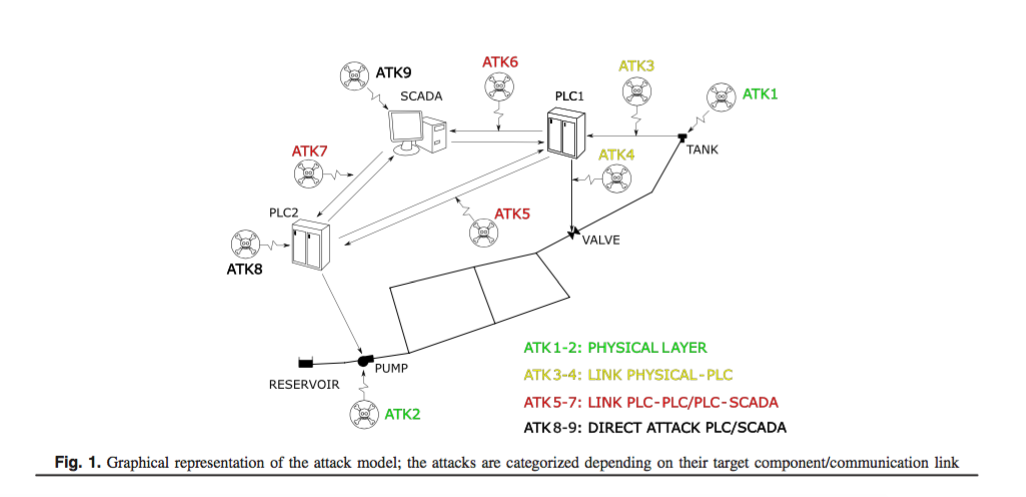


**Focusing on Cybersecurity**

Frameworks and models are helpful for understanding risk, however there must be data on the different components of risk – threats, vulnerabilities, and impacts – to make use of the frameworks. Research on threats to the water sector includes a combination of threats from natural disasters, accidents, and intentionally malicious actions. Amongst this generalized research is a smaller subset focusing specifically on intentionally malicious actions caused by cybersecurity threats. This subset of research on cybersecurity threats to the water and wastewater systems sector has been aimed at justifying the need to focus on cybersecurity (Clark et al, 2017; Dakin, Newman, and Groves, 2009, Johnson and Edwards, 2007) rather than as a guide for better understanding the threats in general.

Previous incidents in the water sector have been identified that show the overall risk to the sector. A study that is cited in several research paper, including Abrams and Weiss, Rao and Francis, and Dakin, Newman, and Groves is an incident at the Maroochy Shire Collection and Treatment System in Queensland, Australia, in which hundreds of thousands of gallons of raw sewage were dumped into nearby water bodies by a former employee who gained remote access to the control systems (Abrams and Weiss, 2008; Rao and Francis, 2015; Dakin, Newman, and Groves, 2009). A series of cyber incidents at a plant in Boca Raton, Florida, are also cited as a reason for increased cybersecurity and monitoring of cyber systems in water plants, as the cause of the incident was never identified due to a lack of monitoring (Horta, 2007; Taormina et al, 2017).

A study conducted by a group of security researchers from Israel focused on a series of simulated cyberattacks against water distribution systems to show the potential for disruption in drinking water supplies (Taormina, et al, 2017). The study provided concrete examples of how cyberattacks could have physical consequences in the water sectors. Their research involved identifying and visualizing how physical systems would be targeted, which contributes greatly to the ability of plant operator without a background in cyber attacks to understand the nature of the information they are conveying. An example of an attack scenario the researchers developed is shown below.



There are some shortcomings in the existing threat-based approaches to security however. One issue that was identified is that existing cybersecurity standards are made to apply to all critical infrastructure sectors and operations, regardless of location, size, or specific equipment used (Morley, 2009). Many of those factors that are overlooked are in fact critical components to understanding the risk to water facilities and should be taken into account when determining risk. Claudia Copeland, a researcher for the Congressional Research Service identified that a small number of large drinking water utilities provide drinking water for over 75% of the population (Copeland, 2010). These facilities have a higher number of components, a higher rate of flow, and a higher risk of being targeted by malicious actors. Their security needs are different from a smaller, rural utility dealing with a different set of problems.

In addition to having different problems, there are also difference in the resources available between large, urban utilities and smaller utilities, both from a staffing and a budgetary perspective. AWWA has also tackled the issue of identifying vulnerabilities specific to the water sector through a tool called the Cybersecurity Guidance Tool, which creates a list of cybersecurity controls based on utility characteristics (Rao and Francis, 2015). This tool evaluates a variety of factors including whether access is local or remote, nature of the connection to remote sites, and other factors that help to narrow down the scope of vulnerabilities and security needs. When combined with the RAMCAP framework, the Cyber Security Guidance Tool can help overcome some of the shortfalls of a one-size-fits-all methodology. There are still gaps in the recommendations generated by using these tools and frameworks, most notably that the guidance is generic and applies primarily to end user computers and not specialized equipment. An example given by Rao and Francis, who completed a robust analysis of literature related to water sector cybersecurity as of 2015, is that a vulnerability identified was “poorly secured legacy systems” and the guidance was “update legacy systems” (Rao and Francis, 2015). This recommendation does not provide guidance on how to initiate the process of updating the systems, what the legacy systems should be updated to, how much updating the systems would cost, or how to prioritize updating legacy systems against other identified vulnerabilities. In short, this research gives water sector owners and operators a starting point, but does not provide information to help with the task of mitigating vulnerabilities.

**Operational Security Needs in the Water Sector**

Another gap in the current literature on cybersecurity in the water sector is a lack of consideration in the operational needs of water and wastewater facilities. Sorlini, et al wrote a paper on methodologies to optimize operations in water facilities, stating that “…drinking water treatments have become more and more complex due to the deterioration of supply sources and the implementation of more restrictive legislation limits” (Sorlini, et al, 2015). Studies on vulnerabilities in the water sector do not always take into consideration the operating requirements of the facilities, including emergency response procedures. One report on security vulnerabilities in 30 drinking water utilities in Virginia conducted by analysts from Booz, Allen, Hamilton identified papers with computer names and passwords taped to computer systems as a cybersecurity vulnerability (Nobel, et al, 2017) and recommended that they be removed and all systems have unique, complex passwords. While this is considered a security best practice for many information technology networks, it does not address the needs of expedient access to systems in the case of an emergency. Security guidelines and recommendations should be designed to work with the unique needs of the sector.

Research into cybersecurity threats and requirements for the water sector thus far have focused primarily on drinking water and, more specifically, water distribution (Clark et al, 2017; Darkin, Newman, and Groves, 2009; Rao and Francis, 2015; Nobel et al, 2017, Taormina, et al, 2017). Threats to this sector are significant, however drinking water is only part of the water systems sector. Wastewater treatment systems are also a critical part and keep the water systems free from contamination that could cause massive outbreaks of disease, and involve many chemical reactions and biological processes which have destructive consequences when not properly managed (Copeland, 2010). It is necessary to develop a solid understanding of these chemical and biological processes, as well as the technology that is used to facilitate and monitor the processes in order to properly identify how to both secure and prioritize security efforts in this sector. In addition, technological advances are being made to innovate and modernize the water treatment sector (Dürrenmatt and Gujer, 2012; Ou, et al, 2015) including the development of smart sensors, artificial neural networks, and artificial intelligence. These systems will introduce new capabilities in the sector, however they will also introduce new cybersecurity risks which can be identified ahead of implementation if they are analyzed from a security perspective.

**Preparing for Cyber attacks**

Researchers have questioned whether the water sector has prepared itself adequately to protect itself from cyber-attacks (Mathews, 2008; Morley 2009; Rao and Francis, 2015). Mathews and Morley both believe that efforts undertaken by the government to secure the water sector have been too focused on terrorist attacks and not enough on other potentials security concerns (Mathews 2008; Morley 2009). Mathews voiced concerns that the individuals who were involved in the creation of the security policy do not fully understand the unique needs of the water sector. He wrote that to ensure that systems are protected, guidance needs to be amended by individuals with a better understanding of the true threats and vulnerabilities of the water sectors, which is why this research will focus on both water systems operations and cybersecurity threats. AWWA published guidance on securing process control systems in water environments, however at the time that the guidance was published there was not a clear understanding of the specific cyber threats to the industry (AWWA, 2017). A major gap in the literature on cybersecurity needs to the water sector has been a focus on cyber threats themselves.

Cyber threats are actors with the intent, capability, and opportunity to impact a computer network. A true threat exists when all three of these aspects are present. An adversary must have a reason to target a system in the water sector, that system must have some sort of vulnerability that presents an opportunity to the adversary, and the adversary must have the capabilities or tools to leverage that opportunity. The current literature on cybersecurity threats to the water sector focuses primarily on the opportunities presented, and very little on the intent of adversaries in targeting the water sector. Some articles make assumptions about what an adversary would or wouldn’t do (Lewis, 2002) and some focus on what an adversary might do based on what attacks are possible within a network (Taormina, et al, 2017) however there has not been a comprehensive analysis of actual attacks against critical infrastructure, their goals, and how those may be applied to the water sector. There is also a gap when it comes to research on capability and opportunity pairings in the water sector. This type of research would focus on the vulnerabilities present in technologies used in the water sector, whether they are vulnerabilities within the system components themselves or vulnerabilities introduced by processes or the implementation of these systems, and then identify if there are tools or capabilities present to leverage those vulnerabilities for malicious purposes. It would also focus on the difficulty level of leveraging the capabilities against opportunities. This analysis would help to prioritize the security efforts of owners and operators within the water and wastewater sectors and round out the information available on risk management in these sectors.

Security relies on an understanding threats and the risk that those threats present. Without understanding these things, security measures may be applied where they are not needed or places where measures are needed may be overlooked. Several frameworks have been created to better understand risk, and although they were not originally created to address the risk presented by cybersecurity threats they can be modified to account for the requirements of protecting an entity from network attacks along with physical attacks.

There are two primary factors to understanding cybersecurity risks that are fundamentally different from their physical threat counterparts; the nature of the threat and the nature of the vulnerability. Cybersecurity threats are defined as an adversary with the intent, capability, and opportunity to cause harm to computer networks. Vulnerabilities are flaws or weaknesses in computer software or hardware that allows the systems to be used in ways that were not intended, and provide the opportunity aspect in the definition of a threat. Vulnerabilities contribute to threats when there is a capability that can be leveraged against it and an adversary with the intent to leverage it.

A major challenge in cybersecurity risk assessments is that both threats and vulnerabilities are more difficult to detect and analyze compared to their physical counterparts, and without firm guidance operators are left to use their own assumptions about both variables when assessing risk. Risk fundamentally relies on an understanding of threats and vulnerabilities. In this research risk is the dependent variable and threats and vulnerabilities are independent variables that influence risk.

**Theoretical Framework**

The goal of this research is to identify which cybersecurity threats pose the greatest risk to the stability and security of technologies in the water industries and how those threats can be mitigated. The NIST Cybersecurity Framework relies on the knowledge of those individuals using it to conduct a risk assessment, and in many cases requires those individuals to have strong understanding of cybersecurity threats and vulnerabilities. If the wrong threats or vulnerabilities are used in the analysis, then the outcome will not support better security. It becomes critical then, to ensure that the threats and vulnerabilities to the water sector are clearly understood so that utility owners and operators can leverage resources such as the NIST framework.

In order to provide information needed to support other cybersecurity specific frameworks, this research will use something more familiar to individuals in the water sector, the Risk Analysis Management for Critical Asset Protection (RAMCAP) framework. This framework was developed in partnership with the American Water Works Association (AWWA) to identify and mitigate risks associated with terrorist attacks after September 11th. The RAMCAP standard is a theoretical framework designed to evaluate the risks and resilience of water sector facilities to man-made and natural hazards, and the framework is well suited for analyzing other threats as well.

The RAMCAP method has seven steps:

1. Asset Characterization to identify critical assets
2. Threat Characterization to determine which threats or hazards to address
3. Consequence Analysis to determine how serious the loss of an asset due to a threat would be
4. Vulnerability Analysis to determine what vulnerabilities would allow a threat or hazard to impact an asset
5. Threat Analysis to determine the likelihood of a threat impacting the overall organization
6. Risk/Resilience Analysis to determine the risk of a threat impacting an asset and how quickly the system would recover
7. Risk/Resilience Management to determine what needs to be done to mitigate a risk and increase resilience

This process provides a sound basis for analysis of cybersecurity threats, however there will need to be some changes made to individual steps to make the framework more conducive to cyberattacks as opposed to terrorist attacks. The primary modifications will need to be made in Steps 2 and 4, threat characterization and vulnerability analysis.

Step 2 in RAMCAP, Threat Characterization, currently consists of man-made hazards, accidents, natural hazards, and dependency hazards such as hazards that affect the supply chain. Under man-made hazards, threats from cyberattacks are currently listed, however they are still characterized as terrorism-based attacks and focus on two primary intentions – destruction and theft of information to facilitate destruction. This research will address these threat characterizations and will also create new threat characterizations by increasing scope of cyberattacks to include threats for financial gain, secondary targeting, hacktivism, and collateral damage from a separate attack. These threat characterizations will be developed by analyzing attacks in the past that have been reported and have impacted utilities. Threat characterization will include direct targeting, where a threat actor intentionally targets a utility, and untargeted threats, where a utility is impacted even though it was not specifically targeted. Accessing information on previous attacks is not an easy process as many utilities do not want to share sensitive information, so this information will be based off case studies that have been published and anonymized data provided by the Department of Homeland Security (DHS) and the Information Sharing and Analysis Center (ISAC) for the water sector.

Step 4 of RAMCAP -Vulnerability Analysis – will also need to be modified to analyze vulnerabilities in computer systems hardware and software. RAMCAP currently recommends that fault analysis, event-tree analysis, path analysis, vulnerability logic diagrams, computer simulation methods, or expert judgment rules-of-thumb be used. This research will leverage the Common Vulnerabilities and Exposures database and the Common Weakness and Exposure database to identify vulnerabilities and weaknesses in systems used in water sector systems. Both databases capture information on vulnerabilities identified using computer simulations and fault analysis. The CVE database is maintained by Mitre and is located at https://cve.mitre.org/. The CWE database is also maintained by Mitre and is located at https://cwe.mitre.org/. Both CVE and CWE information is also maintained in the National Vulnerability Database maintained by NIST, the National Institute of Standards and Technology and is located at https://nvd.nist.gov/. Vulnerabilities specifically identified in industrial control systems are also reported through the Industrial Control Systems Computer Emergency Response Team (ICS-CERT).

The vulnerabilities that are present in hardware or software systems used in water facilities will be further evaluated to understand what opportunity they are presenting the adversary. Some vulnerabilities allow access to systems, and others allow someone who already has access a way to get more permissions to carry out malicious activities. Some vulnerabilities enable a denial of service against the system and some allow an adversary to steal information. These details about vulnerabilities are important to understanding the risk that they present.

With a better understanding of the independent variables of threats and vulnerabilities of cyberattacks in the water and waste water sectors, it will be possible to complete the RAMCAP analysis for cybersecurity threats and determine which threats provide the greatest risk. That understanding will allow water sector owners and operators to better leverage additional standards and frameworks such as the NIST Cybersecurity Framework and enable them to apply the best security mitigations to address their risk.

Many water and wastewater utilities understand that there is risk associated with cyber attacks, however the details around what that risk is and how it should be prioritized and addressed are more difficult to articulate. While organizations such as the Environmental Protection Agency have created guidelines and checklists to help water utilities start to address these risks, the checklists often have a single line that says “Identify the most significant threats to the sector” and “identify vulnerabilities” (EPA, 2016). More detailed information on threats and vulnerabilities specific to the water sector is difficult to find or exists behind a pay-wall that many smaller or municipal utilities do not have the funding to access. The goal of this research is to provide the information on threats and vulnerabilities to assist organizations in the water and wastewater sectors with better assessing their risk. Threats and vulnerabilities are not static and will change over time, so both the specific findings as well as the methodology used will be explained in detail so that it can be replicated in the future if needed.

**Methodology**

This research utilizes a mixed method methodology, and includes both qualitative and quantitative aspects. The dependent variable is the risk to the water sectors from cyber attacks. The independent variables are threat characterization, vulnerability characterization, and resilience of technology systems in the sector. When the three independent variables are evaluated, they can be measured using the RAMCAP framework, Risk Management Analysis for Critical Asset Protection. This framework was developed in coordination with the American Water Works Association to determine overall risk and therefore is a framework that many water and wastewater sector organizations are already familiar with. As water sector organizations strives to improve the efficiency, safety, and security of its infrastructure to ensure clean water is available for industrial, commercial, and residential use, this research will help to understand and account for the rising risks associated with cyber attacks.

Threat characterization includes the intent, capabilities, and opportunities of an adversary targeting the water and wastewater sectors. Because the focus is on the human element this variable is studied using qualitative methods. Threats are evaluated by looking at how similar threats have previous manifested themselves, both in the water sector and in critical infrastructure sectors that use similar technologies. To achieve this, the research uses case studies on previous cyberattacks in these sectors to identify when, why, and how adversaries target critical infrastructure. Case studies such as the Maroochy Shire insider cyber attack, a cyber attack on a water plant in Illinois, and multiple cyber attacks on a water plant in Boca Raton, Florida will be used to identify attacker motivations, as well technical details on how they carried out the attack. Additional case studies outside of the water sector are also used, and include attacks on Safety Instrumented Systems (SIS) in the energy sector that are also similarly used in the water sectors (Dragos, 2018a). Case studies on ransomware and denial of service attacks that impacted the water sector as well as other, unrelated sectors are also used as examples of untargeted or opportunistic threats. The result of this research is a series of threat characterizations detailing the combinations of intent, capabilities, and opportunities leveraged by adversaries. Each threat characterization will also include a rating on the likelihood of the threat manifesting based on the nature of the intent, the sophistication of the attacker, and the difficulty to technically carry out the attack.

Quantitative methods are used to evaluate the vulnerability and opportunity aspects of threats to technologies in the water sector. This will be done by calculating the severity and ease of exploitation using the Common Vulnerability Scoring System (CVSS) associated with the Common Vulnerability and Exposures (CVEs) and Common Weakness and Exposures (CWEs) of technologies in the water sectors.

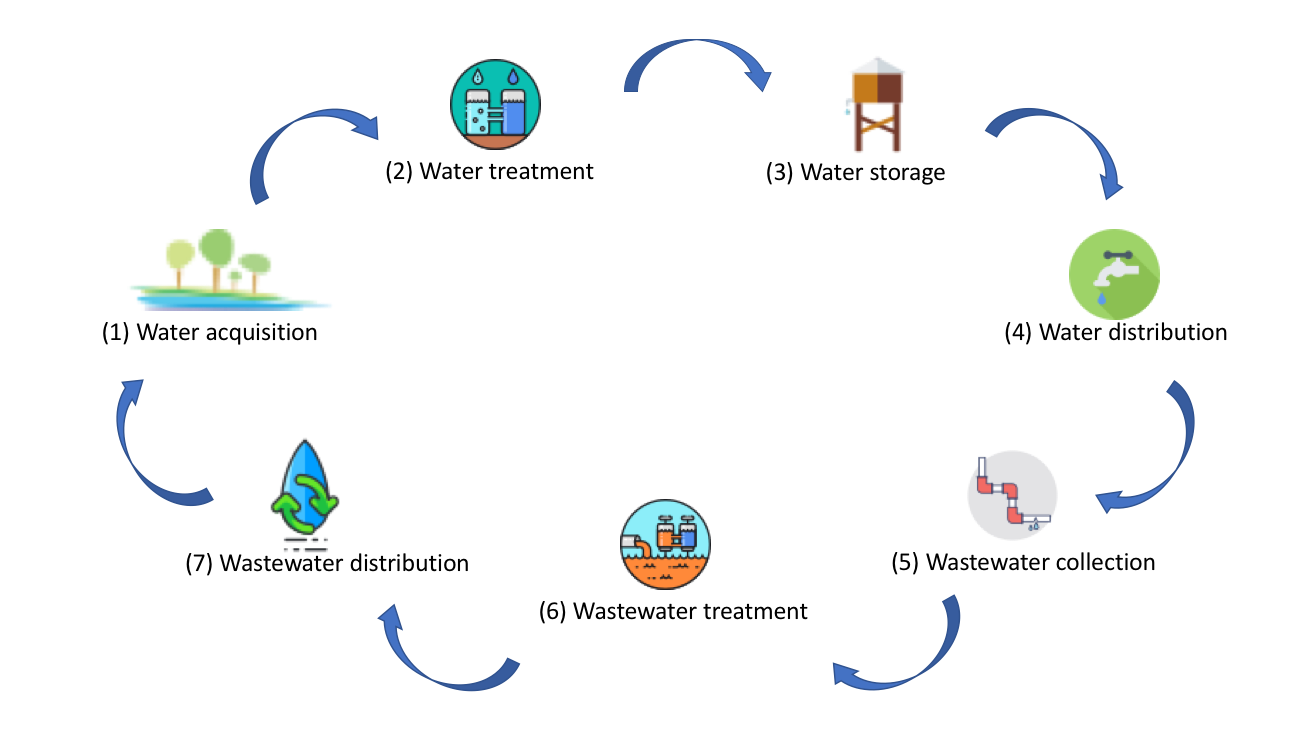
This aspect of the research will be done with a technology-centric focus. The primary manufacturers of technologies in the water and wastewater sectors are Rockwell Automation, Siemens, Emerson, Hach, ADD, CSIA, and Honeywell, and research focuses on the vulnerabilities the products made by these manufacturers. The vulnerabilities in technologies will be evaluated against research on cybersecurity threats to identify whether adversaries likely have the intent, capability, and opportunity to carry out an attack that would impact water and wastewater systems stability and security. According to ICS-CERT, over 90% of vulnerabilities are reported by security researchers, who often research vulnerabilities as either a part of their job or as an additional duty (ICS-CERT, 2016). Many vulnerabilities then go through coordinated disclosure, and often the vulnerabilities will not be disclosed until there is a patch or a fix. Because of this, there are likely to be vulnerabilities present in technologies that have not been reported, and therefore are not within the scope of this research. Likewise, there are cyber attacks and intrusions in water and wastewater systems that have not been reported, either publicly or privately, and cannot be evaluated. This research is based on the best available information. As new information emerges the same research methodology can be used to produce new threat and vulnerability characterizations as needed. The development of not just baseline threat and vulnerability characteristics, but of the methodology to analyze new threats and vulnerabilities will support water and wastewater systems sector operators in their role of providing clean, reliable water to support daily life.

**Results**

The goal of this research is to identify which cybersecurity threats pose the greatest risk to the stability and security of technologies in the water industries. Cybersecurity threats are defined as adversaries with the intent, opportunity, and capability to carry out an attack using cyber means. Risk is calculated by identifying the threats, vulnerabilities, and the impact of an adverse action. The water sectors, both drinking water and waste water, are familiar with conducting risk assessments to account for natural disasters, accidents, and physical attacks. The same fundamental process can be used to address cybersecurity threats, however additional variables on the nature of cyber threats and vulnerabilities must first be identified. This research will identify these variables and demonstrate how they can be used to address cybersecurity risk in the incredibly complex water systems sector.

**The Water and Wastewater Systems Sector**

There are over 155,000 public water systems in the United States, ranging in size from hundreds of consumers to millions (RCAP, 2011a). These systems are not only numerous; they are complex as well. The reason that the water industries are called the “water systems sector” is that they are made up of many different systems with specific roles and functions that operate in a cyclical nature, known as the water cycle. An example of the different systems involved in the water sector generated as a part of this research is shown below.



The water intake system (1) acquires water, primarily from ground water or surface water. Ground water procurement involves drilling and maintaining wells. Ground water typically has less containments than other water sources, such as surface water. Surface water is water that is collected from rivers, streams, reservoirs, or oceans. Surface water must be more heavily treated than ground water because of the increased risk of contamination, which means that there is often more equipment involved in the testing phase, which occurs in the water treatment systems. Pumps are used to get the water to the water treatment facilities.

The water treatment system (2) ensures that water is safe to drink, and includes processes for testing, treating, and disinfecting water (RCAP, 2011a). Ground water systems require less treatment than surface water. In many cases the only treatment needed with ground water is the addition of chlorine disinfectant. Surface water treatment is more complex. The first step is pre-settlement, where the water sits while larger sediments settle to the bottom of the tank. Chemical coagulants may be added to the water to expedite the settlement process.

The next step is pre-treatment, where chemicals such as chlorine or potassium permanganate are added to the settled water to oxidize contaminants. Mixers are used to ensure that pre-treatment chemicals are dispersed properly in the water. After it is mixed, the water goes through two processes known as coagulation and flocculation, which facilitates the binding of smaller particles of dirt or other organic matter together so they can be more easily removed (Heinzmann, 1994). These systems employ slow turning paddles to help the particles bind together in ideal sizes to be removed. After flocculation, the water is pumped into tanks to allow the sediments to settle to the bottom once again. Sediment is pumped to a sludge basin, where it is often then pumped to the sewer system.

The water is then fed through a filtration system to remove any remaining particles. There are many different types of filter: sand filters, membrane filters, cartridge filters, pressure vessel filters, bag filters, or diatomaceous earth filters. The filters have varying degrees of technology involved; many filters use gravity, reverse osmosis, or other natural processes, however some, like pressure vessel filters, require equipment to support the filtration process (RCAP, 2011a).

After filtration, post-processing chemicals are added to the water. Post-processing chemicals disinfect and destroy disease-causing organisms. Chlorine, chloramines, and ozone are the most common chemical used at this stage. Ultra-violet light is sometimes used to disinfect, which requires special UV light systems at this stage of the process. The water quality is tested at many different stages of the treatment process using a combination of manual and automated systems. At the end of the treatment process the water is moved into water storage using pumps. Water storage systems (3), such as reservoirs or tanks, store water until it needed and ensure that demand can be met during peak times. Water that is being stored must still be tested to ensure that no containments have been introduced (Ibid.,).

The water distribution system (4) moves water from the storage systems to the customers who will use the water. The first water distribution systems relied exclusively on gravity, and therefore the water source needed to be at a higher elevation than its customers (Sedlak, 2014). Modern water distribution relies heavily on pumps to get water to its destination. There are three types of pumps commonly found in water distribution systems: centrifugal pumps, vertical turbine pumps, and submersible pumps.

Pipes are used to carry water from the treatment plant or storage systems to the end-users. A series of valves regulate the flow of water along the pipes. Some valves are simple with an on/off capability, and some are more complex and use technologies such as microprocessors to adjust water pressure or temperature. Additional disinfectants are sometimes added to the water during distribution, typically when water is traveling long distances and the original disinfectants dissipate. In these situations, additional pumps and valves are needed to add chemicals to the water that is in transit. As water arrives at its destination there are often meters used to utilities to measure the amount of water than it used by the end-user do the user can be charged.

Once water has been used, the byproducts become part of the wastewater system. Water gets to a treatment facilities via a wastewater collection system (5), also known as a sewage system. Sewage systems use gravity as much as possible, however when it is not possible to use gravity alone, lift stations are utilized to maintain the necessary flow rate. Lift stations include pumps, a power supply, a control system, and ventilation. Valves control flow rates along the way, and sampling stations analyze the quality of the water as it travels to the treatment plant. Once water arrives at the plant it goes through a series of physical filters to remove trash and other large materials which are typically taken to a landfill. After that the treatment process begins.

The wastewater treatment system (6) removes contaminants from used water, preventing it from further polluting surface and ground water and often allowing it to be reused as non-potable gray water for irrigation and industrial purposes (RCAP, 2011b). Bacteria and pathogens are often present in wastewater and can cause widespread illness if not properly treated. The treatment process has four steps, pre-treatment, primary treatment, secondary treatment, and disinfection. In pre-treatment, large materials such as tree branches or garbage are removed uses screens. The screens must be cleaned to allow continual flow of wastewater into the systems. Some facilities do not use screens to remove these larger materials, and instead use a grinding process to reduce the size of the materials so they can be handled later in the process. Grinders use mechanical equipment known as macerators or hammermills. Flow equalization is also part of pre-treatment (Ibid.,).

During times of high volumes of wastewater, some of the wastewater will be moved into a holding basin, where pumps will release it into the treatment facility in a controlled manner to avoid overwhelming the systems (Heinzmann,1994). Without flow equalization, the treatment facility could become overwhelmed during wet weather or storms which would result in an inability to properly treat the water.

Once wastewater has been properly treated it enters the wastewater distribution system (7) that transports water to streams or other surface water bodies, where it will be treated along with other surface water or will be used as part of an approved irrigation system for wastewater effluent. Solids that were removed from the wastewater, often referred to as sludge, still need to be dealt with as well. In the sludge disposal system (8) sludge is treated through processes such as thickening, dewatering, conditioning by adding chemicals, and stabilizing the solids. The final product is then disposed of in landfills, used as compost, or burned in systems such as incinerators or gas systems which produce energy (RCAP, 2011b).

It is important for cybersecurity professionals to have an understanding of the complexities of the water sector so that they can provide specific guidance on where the most significant threats exist, or identify when a vulnerability is found is a critical portion of a system. Water systems are very different from traditional business networks that are often evaluated, and a lack of understanding of the differences has contributed to previous generic guidance. Cybersecurity professionals must be familiar with the water systems as well as the different technologies that are used to keep they systems functioning properly.

**Technologies in the Water Sector**

There are many different technologies that support the processes in the water sector, and the majority are classified as Industrial Control Systems. According to the AWWA’s Water Security Roadmap, Industrial Control Systems are “…computer based facilities, systems, and equipment used to remotely monitor and/or control critical process and physical functions. These systems collect data from the field, process and display this information, and then, in some systems, relay control commands to local or remote equipment.” (AWWA, 2008).

In some cases, Industrial Control Systems are specific to the water systems sector, but often it is a common component used in many different industries. Pumps are one example of ICS used in the water sector that is also present in many other industrial operations. Pumps are critical in nearly every system in the water sectors, from water acquisition to treatment, to distribution, to waste water reclamation, treatment, and disposal. Ground water systems rely on mechanical pumps such as electric submersible pumps or vertical turbine pumps to draw the ground water to the surface.

In smaller water systems, there are often not backup pumps present, making these pumps critical to operations. Small systems also have less stored water, which means that a pump failure can cause water shortages in matters of minutes (RCAP, 2011a). Surface water also relies on pumps, primary suction pumps that draw water in from rivers and streams. Pumps are used to move water between different tanks and processes in both drinking water treatment and waste water treatment, and are also used to add chemicals and disinfectants to the water.

Probes and sensors also play a critical role in many aspects of water treatment and distribution. These devices allow for greater automation at water systems sector facilities by performing a variety of tests that were previously done manually. Water temperature, PH, and quality used to be tested manually by plant operators, but this can now be done on a reoccurring basis by technologies, with the operators validating the work. In many cases the validation is done with SCADA systems. Supervisory Control and Data Acquisition (SCADA) systems are used to monitor processes across the water cycle, capturing information about the performance and operations of the equipment and the processes that they control.

Nearly every industry that leverages Industrial Control Systems have SCADA systems to operate and manage them (AWWA, 2008). The water sector also relies on different systems to ensure that all the moving parts are operating safely. These systems are called Safety Instrumented Systems, and are present in many systems, including treatment and distribution (Dragos, 2018).

Some equipment is specialized to the water systems sector. Devices such as oscillating flocculators, dissolved air floatation systems, and specialized sewage blower systems are less common outside the water and wastewater systems sector. Threats against industrial control systems that are present in many sectors have the potential to impact the water system, even if water is not the primary or initial target of an adversary, however targeting of technologies that are unique to the water sector show a more specific intent to cause harm in this specific sector. In order to understand the intent threat aspect and develop threat characteristics, it is important to understand when and how the water systems sectors were previously targeted, which portion or portions of the water cycle were impacted, and what technologies were targeted as part of an attack.

**Threat Assessment**

Reports of cyber attacks against critical infrastructure are increasing, resulting in more case studies that can be used to understand the threats. Cybersecurity threats are adversaries with the intent, capability, and opportunity to carry out an attack using cyber means. Case studies can help to understand not just what happened in an attack against a system, but what the adversary’s goals and motivations were.

One of the most cited case studies in water sector cybersecurity is the Maroochy Shire Sewage Collection and Treatment System in Queensland, Australia. This attack occurred over a two-month period in 2000 and resulted in the spillage of over 200,000 gallons of raw sewage into surrounding water bodies (Panguluri, Phillips, and Cusimano, 2011). The attacker was a former employee who was able to gain unauthorized access to the Sewage Treatment Plant’s SCADA systems and send commands to release sewage before it had completed the treatment process. The attacker had helped design the plant and had taken equipment and software from the facility, which he used to gain access to the systems (Denning, 2012). In this case, the adversary’s intent was to cause damage to the system for personal reasons, the capability that were leveraged was the equipment taken from the facility and used to control the systems, and the opportunity that was leveraged was the system knowledge and access.

A second case study involves an intrusion at a utility in Boca Raton, Florida, with a water and wastewater facility collocated. According to a senior systems analyst and controller for the city of Boca Raton, there was a series of cybersecurity incidents at the plant that resulted in a shutdown of the SCADA system controlling plant operations (Horta, 2007; Taormina et al, 2017). The water facility did not have systems in place to monitor what was happening on their systems, so there is an unfortunate lack of detail about what occurred.

A 2011 incident at an undisclosed water utility in Springfield, Illinois, was described as the first cyberattack known to damage a critical infrastructure system in America (Nakashima, Nov 18, 2011). In this case, attackers first compromised a software company that had a database of usernames and passwords of control systems that run in the water plants. The information provided about the incident did not detail what software or what passwords were stolen, however many industrial control system manufacturers have default user names and passwords set for maintenance purposes, and those may have been the passwords that were stolen (Ibid,.). The adversary then used the stolen credentials to gain access to the control systems at the utility, which had to be exposed to the internet in order for the attackers to access them. The attackers maintained access for several months, and during that period frequently interfered with operations of water pumps. One of the pumps subsequently burned out after being turned on and off in quick succession. The reports do not detail which water system the pumps were in, and water pumps are present in nearly every system in the water sector which. While the attacks resulted in damage, it is not clear whether the damage was the adversary’s intent or whether it was accidental. The nature of the activity may have been testing or even mischief, however the result was damage.

An incident in 2011 involved a hacker who gained access to a wastewater treatment plant in South Houston, Texas (RISI, 2018). The hacker identified a three-character password that was used to secure the SCADA system of the facility. In this case the system was a Human Machine Interface (HMI) that allowed an operator to control different systems, such as valves, pumps, and motors. In this case the hacker did not tamper with anything, but wanted to prove a point about the lack of security in critical infrastructure and posted pictures online showing the access that they gained and what they could have done with the access, including speculation that they could have changes settings, turned off different pieces of equipment, or locked other users out of the systems (Ibid.,).

Another case study of a cyber attack at a water facility came from the Verizon Data Breach Digest in 2016 (Verizon, 2016), where the Verizon Incident Response team investigated an intrusion. In order to protect the utility, they released all of the information using a fictitious name, the Kemuri Water Company. The information technology staff of the water company had identified suspicious activity over the past few months. There had been an unexplained pattern of activity with the valves and ducts that controlled the amount of chemical disinfectants added to the water at the final stages of drinking water treatment. There had also been problems with the valves controlling the water flow rate, resulting in water distribution interruption.

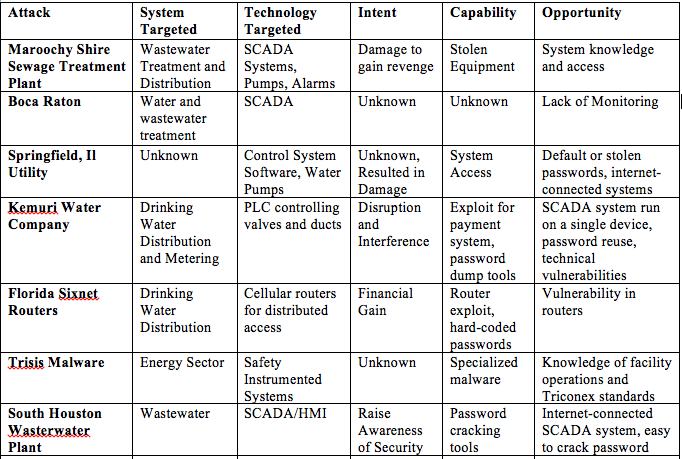
After an investigation, the research team identified that an adversary identified as a hactivist group, an ideologically motivated adversary often carrying out activities to support or draw attention to a cause, usually by disrupting and denying access to computer systems. The adversaries obtained access to the system through a vulnerability in an internet-accessible payment system, which was connected to the company’s SCADA system. The adversaries used credentials stolen from the payment system to gain access to the SCADA systems and modify the application settings that controlled the chemical distribution and flow control. The investigator wrote that the adversaries seemed to have little knowledge or experience modifying the settings, but were still able to have an impact.

Not all incidents reported in the water sector involve the compromise of control systems; a case study of an undisclosed utility in Florida detailed how the utility’s bandwidth was the actual target of the adversaries. In this example, adversaries were able to exploit a weakness in the cellular Sixnet routers the utility used for communications between their remote water distribution sites. The weakness was a hardcoded username and password present in every Sixnet router, which the adversaries used to simply log on to the device. The adversaries gained control of four of the utility’s seven routers and used their bandwidth, incurring tens of thousands of dollars in charges for the utility (Circle of Blue, 2017). The bandwidth usage did not appear to have negatively impacted operations; however this case study illustrates how easy it would be for an adversary to disrupt communications between remote facilities in the water sector.

A case study involving the energy sector impacted equipment that is used in the water sector. In late 2017 an incident response company specializing in Industrial Control Systems identified a new piece of malicious software, known as malware, that targeted Safety Instrumented Systems (SIS) used to protect systems in the case of equipment malfunctions (Dragos, 2017). This malware targeted a very specific SIS technology, the Triconex model created by Schneider Electric. The Triconex line of products is used in the energy sector, water systems sector, oil and gas, and manufacturing sectors, although there are variations in the systems depending on the industry they are being used in.

Trisis malware is a second-stage malware used specifically to manipulate control systems. Adversaries first had to gain access to the network and then connect to the SIS engineering workstation to carry out the attack. When the adversaries attempted to reconfigure the SIS code, the system’s built-in redundancy identified the change and shut down to a failed safe state as they are designed to do (Fireye, 2017). Researchers assess that this was a mistake on the part of the adversary. The adversary demonstrated a high level of sophistication and understanding in the development of this malware, and it is likely that they will continue to perfect this attack method. Compromising the SIS in any critical infrastructure facility can allow the adversary to put other physical systems such as incinerators used in sludge disposal into an unsafe state resulting in significant damage.

After the analysis of the previous case studies was conducted, a matrix was developed as a part of the research to show trends and differences in the various aspects that were analyzed. Below is a matrix capturing the threat aspects of the case studies used in this research.

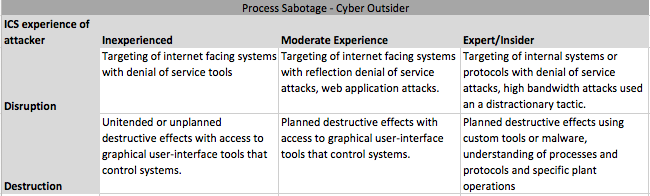
****

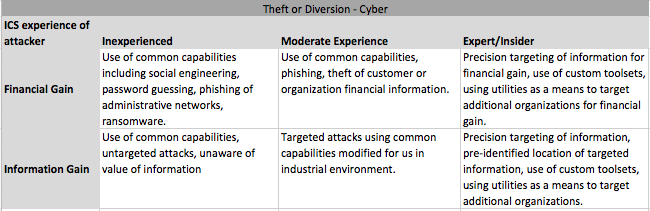
From the case studies, three distinct adversary trends emerge. In some of the cases, such as in the Maroochy Shire incident and the Trisis malware, the adversary had a clear understanding of the Industrial Control System Environment and was able to specify exactly what actions they want to take place. With the Maroochy Shire incident it was due to the knowledge and specialized equipment the previous employee had. In the Trisis case, it was likely a result of a well-funded adversary spending a great deal of time on research and understanding the target system.

A second pattern that emerges is adversaries such as the ones targeting the Kemuri Water Company and Springfield utility who do not have ICS experience, but have an impact on the systems by taking advantage of the applications designed to help operators control the systems and essentially trying different methods until something works. A third pattern, present in the Florida Sixnet router compromise, and potentially in the Boca Raton case, is an adversary who is not specifically targeting the water sector to compromise the Industrial Control Systems, and instead has other motivations such as financial gain. An adversary in this situation may end up having an impact on the system without specifically intending to.

Another trend that emerged is the targeting of specific technologies. In the majority of case studies reviewed, the adversaries targeted the SCADA control system or used them as a way to get access to the devices they compromised. This makes control systems especially important to secure. The third trend was the use of passwords by adversaries, either default, hard-coded (built into the system) or stolen from other systems. Internet-connected systems often provided adversaries the opportunity to gain access to networks and compromise the systems.

The current reference threats in the RAMCAP model account for very basic cyber threats fitting into 4 categories: process sabotage from an insider threat, process sabotage from a remote threat, theft or diversion from an insider threat, and theft or diversion from an outsides threat. Using the new information on the nature of threats based on an analysis of the case studies above, it is possible to develop a more robust threat characterization matrix to account for the full range of cybersecurity threats facing the water and wastewater sectors. Updated threat references for use in the RAMCAP process that were developed as a part of this research are shown below.





The updated threat references specify not only the type of attack – a disruptive or destructive attack versus an attack for financial or information gain, but also break down the experience level of an attacker, inexperienced, moderately experienced, or expert/insider, and identify the tactics the adversary is likely to use based on their experience with industrial control systems and their intent.

**Vulnerability Assessment**

The second aspect of risk that needs to be addressed is the vulnerabilities that are present in the water and wastewater systems sectors. A vulnerability is defined as a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” (NIST, 2013). Cybersecurity vulnerabilities typically fall into 2 categories: common vulnerabilities and exposures (CVE) or common weakness and exposures (CWE). CVEs include errors or flaws in the information system’s code that allows it to be used in a manner not originally intended. The only way to remediate a CVE is for the developer of the vulnerable code to identify a way to fix the flaw and then update the code. This fix is referred to as a “patch” and must be implemented everywhere that the vulnerable code was used.

CWEs are weaknesses in the way that the information system or program was designed or implemented that can lead to unintended results. An example is a system that was designed with default hard coded passwords that cannot be changed, meaning that anyone who knows that password can get access to the system, whether the owner wants them to or not. CWEs can also be introduced during configuration, for example an owner configuring a system with a weak password or no password at all. Fixes for CWEs often involve process changes or mitigations rather than changes to the system code itself.

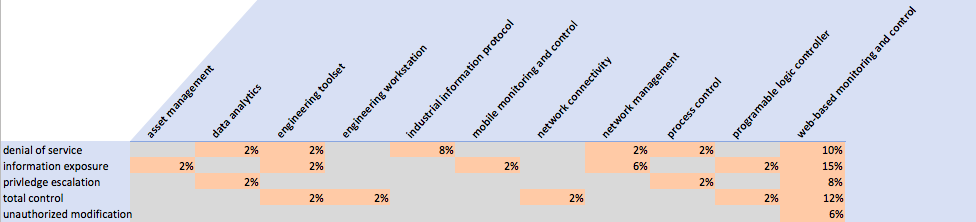
Both CVEs and CWEs have been identified in the water and wastewater systems sector, and were identified in the case studies used to identify threat characteristics. CVEs and CWEs are assigned severity scores based on how difficult they are to take advantage of, what type of access or permissions they give an attacker, whether the vulnerabilities can be exploited remotely (from anywhere on the internet) or whether they can only be exploited locally with an existing connection, physical or logical, to the device. The severity score also account for the impact of a adversary exploiting the vulnerability. In some instances, the adversary would be able to view information, in some cases they would be able to disable the system, and in some cases they would be able to gain total control of the system to make whatever changes they wanted.

The industrial control system-focused cybersecurity firm Dragos conducted a study of all industrial control system vulnerabilities disclosed in 2017 and identified 163 vulnerabilities (Dragos, 2018b). After the vulnerabilities were identified they analyzed the impact of the vulnerabilities, how difficult it was for an adversary to compromise based on location in the network, and what component they impacted. When identifying the impact of the vulnerabilities, they found that 33 percent could result in a loss of view, meaning that the plant operators would not be able to see what was occurring. 29 percent of vulnerabilities resulted in a loss of control of the systems. 28 percent resulted in both a loss of view and a loss of control. In ten percent of vulnerabilities the result was neither a loss of view nor a loss of control (Ibid.,).

It is necessary to build upon existing research to better understand the vulnerability characteristics of systems in the water systems sectors. The report released by Dragos was the first of its nature - there has not been much attention given to understanding the nature of vulnerabilities in industrial control systems to determine which ones are most likely to be exploited by a malicious adversary. Using variables such as location in the network can help to understand how much work an adversary would have to do to compromise the vulnerable system, or how much luck they would have to have that a utility misconfigured their systems as we saw in several of the examples in the case studies.

Just as threat characterizations are used to better understand how an adversary may impact an organization or a facility, vulnerability characterizations are used to understand how they need to be addressed or mitigated, and whether they will support any adversary in their attempt to impact systems. Vulnerabilities can be used by adversaries as opportunities to gain access to networks or to cause damage or disruptions to systems. The primary opportunities leveraged in the case studies used in this research were technical vulnerabilities on web-facing applications and SCADA servers and weak default, or leaked passwords for web applications and SCADA devices.

A review of vulnerabilities reported by the Industrial Control System – Computer Emergency Response Team (ICS-CERT) that the vendors identified as being used in the water and wastewater sector shows that fifty-seven percent of technical vulnerabilities identified in systems used by the water and wastewater sectors involved web-based applications for monitoring and controlling SCADA systems or other control equipment. Eighteen percent of the vulnerabilities in these systems cause a denial of service, meaning that exploiting the vulnerabilities could cause the systems to go offline, reboot, or become unresponsive. Thirty-two percent of web-based vulnerabilities cause information disclosure, and twenty-one percent allow an adversary to gain total control and make significant changes to the systems. Gaining control of a web-based monitoring and control system lets an adversary who is less experienced in industrial control system operations have an impact on the systems, as shown in several of the case studies reviewed previously.



Although an overwhelming number of vulnerabilities have been identified in web-based control systems, there are other systems that also have identified vulnerabilities. Eight percent of vulnerabilities were found in network management systems such as routers or protocol-bridges, six percent were in engineering toolsets that engineers use to design and test control system integrations, and four percent each in data analytics equipment, process control devices, and programmable logic controllers. In addition, seventy-three percent of attacks only required that an adversary have a low skill level to accomplish, and fifty-nine percent of vulnerabilities required a low skill level and could also be done remotely without requiring any previous access to the systems.

Legitimate credentials were the top threat opportunity leveraged by adversaries in documented cases of cyber attacks against the water and wastewater sectors. Sixteen percent of vulnerabilities identified in the water systems sectors involved password errors, including storing and transmitting passwords in plaintext without any form of encryption, default credentials set by the manufacturers, and even hardcoded passwords in control systems. These passwords are designed to be used for development and maintenance purposes, however they cannot be removed from the device once it is operationalized in a facility. These credentials can be used by anyone who knows that they exist. ICS vendors previously stated that the use of hardcoded passwords allowed for better support and introduced little risk, because only the vendors know about them, however in recent years there has been an increase in public knowledge of these passwords, and online repositories of default and hardcoded credentials for ICS equipment have emerged.

Web-based control systems, network management systems, and password related vulnerabilities account for the opportunities that adversaries used to compromise the water systems in the case studies of attacks in the sector. Analysis of the characteristics of these vulnerabilities help to further understand the threat to the water and wastewater systems sector from cyber threats. In additional, over half of the threats analyzed in the water sector were carried out by adversaries with limited or no experience with technologies in this sector. Seventy-three percent of vulnerabilities in technologies in the water sector require only a low level of expertise to exploit them, and while there will always be threats from expert-level or insider threats to be aware of, the most likely threat to cybersecurity in water and wastewater systems sector comes from inexperienced or moderately experienced adversaries leveraging vulnerabilities and weaknesses that require low skill levels to carry out.

**Discussion**

The goal of this research was to identify what cybersecurity threats posed the greatest risk to the water and wastewater systems sectors in order to help facilities in these sectors protect themselves. After an analysis of previous threats that have been seen in the sector and reviewing vulnerabilities identified in technologies used in these sectors, the findings show that threats who are targeting the water sector directly and have either a low or moderate skill level present the most likely and most significant risk to the sector. Adversaries such as those seen carrying out the attack on the plant code-named the Kemuri Water Company had a malicious intent to cause disruption and destruction, had a moderate skill level and were able to access a web-based SCADA system connected to industrial control systems, and we able to use the graphical user interface to cause damage to the facility. Focusing on this type of threat, evaluating weaknesses and vulnerabilities that similar adversaries would exploit, and understanding how an adversary could use internal systems in a malicious way can help water and wastewater systems sector facilities and operators understand how to best protect their networks.

The threat and vulnerability characterizations developed as a part of this research are designed to be an input to a structured risk management process, such as the RAMCAP method used in the water sector or the NIST Cybersecurity framework. The threat characterizations listed on page 42 can be used to assess cybersecurity threats to the water sector, however a utility is not limited to these threats alone. New threats, based on new reports of cyber attacks that are made public or are shared with the utility by trusted parties can be analyzed using the process and matrix that were used to analyze the case studies, as shown on page 39. If there have been previous incidents or attacks at the utility itself, those previous attacks can also be analyzed using the same process and matrix to provide a unique view of the threats facing the specific utility.

Likewise, vulnerabilities that are identified in technologies used in a utility can be analyzed by identifying the type of technology it impacts, whether it can be attacked remotely or if it needs local access, and what the impact of successful exploitation would be. Utilities can self-identify critical system components based on their unique setups and the part or parts of the water cycle that they support, and focus on vulnerabilities in those systems.

With the building blocks of threat and vulnerability characterization and the methodologies and data needed to update these aspects, water and wastewater systems sector owners and operators can better leverage existing risk management frameworks to continually identify and address critical cybersecurity threats.

References:

Abrams, M., & Weiss, J. (2008). Peril in the pipeline. Intech, 55(6), 36-37,40,42.

American Water Works Association (AWWA). (2017). Process Control System Security Guidance for the Water Sector. https://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf (accessed April 8, 2018)

Clark, R., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting Drinking Water Utilities From Cyber threats. Journal: American Water Works Association, 109(2), 50-58.

Copeland, Claudia. (2010) Terrorism and Security Issues Facing the Water Infrastructure Sector. Congressional Research Service Reports for Congress. RL32189.

Dakin, R., Newman, R., & Groves, D. (2009). The case for cyber security in the water sector. American Water Works Association Journal, 101(12), 30-32.

ICS-CERT. (2016). ICS-CERT Annual Vulnerability Coordination Report: 2016. https://ics-cert.us-cert.gov/sites/default/files/Annual\_Reports/NCCIC\_ICS-CERT\_2016\_Annual\_Vulnerability\_Coordination\_Report\_S508C.pdf (accessed April 8, 2018)

Denning, Dorothy E. (2012). "Stuxnet: What Has Changed?" Future Internet 4, no. 3: 672-687.

Dragos. (2018a). TRISIS Malware Analysis of Safety System Targeted Malware. https://dragos.com/blog/trisis/TRISIS-01.pdf. (accessed April 3, 2018).

Dragos. (2018b). Industrial Control Vulnerabilities – 2017 in Review. https://dragos.com/media/2017-Review-Industrial-Control-Vulnerabilities.pdf (accessed April 4, 2018).

Dürrenmatt, David J. and Gujer, W. (2012). Data-driven Modeling Approaches to Support Wastewater Treatment Plant Operation. Environmental Modelling & Software

30, 47-56.

Environmental Protection Agency. 2016. WATER SECTOR CYBERSECURITY BRIEF FOR STATES. https://www.asdwa.org/wp-content/uploads/2016/07/Cybersecurity-Guide-for-States\_Final.pdf. (accessed April 8, 2018).

FIRST. Date Unknown. Common Vulnerability Scoring System v3.0: Specification Document.

https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf. (accessed April 8, 2018).

Heinzmann, B. (1994). Coagulation and flocculation of storm water from a separate sewer system - a new possibility for enhanced treatment. Water Science and Technology, 29(12), 267-278.

Horta, R. (2007). The city of Boca Raton: A case study in water utility Cybersecurity. American Water Works Association Journal, 99(3), 48-50.

Johnson, S., & Edwards, D. (2007). Why water and wastewater utilities should be concerned about cyber security. American Water Works Association Journal, 99(9), 89-90,92,94.

Kamien, D. G. (2006). The McGraw-Hill homeland security handbook: the definitive guide for law enforcement, EMT, and all other security professionals. New York: McGraw-Hill.

Kroll, Dan. (2016). Water Distribution Monitoring: Opportunities and Challenges for Enhancing Water Quality and Security. Hach Corporation. https://www.researchgate.net/publication/228385734\_Water\_Distribution\_Monitoring\_Opportunities\_and\_Challenges\_for\_Enhancing\_Water\_Quality\_and\_Security

Lewis, James. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf> (accessed April 7, 2018)

Mathews, Robert. (2008). “National Security Strategy for Water”. *Engineering in Medicine and Biology Magazine*, IEEE, Vol 27, Issue 6: 42-53.

Morley, K. M. (2009). “An Evolving Culture of Security and Preparedness in the Water Sector”. American Water Works Association Journal, Vol 101, Issue 1: 32-35.

Morley, K.M. (2010). “Advancing the Culture of Security and Preparedness in the Water Sector” American Water Works Association. Journal; Jun 2010; 102, pg. 34

Muller, M.,Pr Eng F.S.A.I.C.E. (2017). Understanding the origins of cape Town’s water crisis. Civil Engineering : Magazine of the South African Institution of Civil Engineering, 25(5), 11-16.

National Institute of Standards and Technology. (2013). Glossary of Key Information Security Terms, Revision 2. https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. (accessed April 8, 2018).

National Institute of Standards and Technology. (2014). NIST Cybersecurity Framework. https://www.nist.gov/cyberframework (accessed April 8, 2018).

Noble, T., Manalo, C., Miller, K., & Ferro, C. (2017). Cybersecurity assessments of 30 drinking water utilities. Journal of the New England Water Works Association, 131(4), 219-227.

Ou, H., Wei, C., Wu, H., Mo, C., & He, B. (2015). Sequential dynamic artificial neural network modeling of a full-scale coking wastewater treatment plant with fluidized bed reactors. Environmental Science and Pollution Research International, 22(20), 15910-15919.

Panguluri, S., Phillips, W., & Cusimano, J. (2011). Protecting water and wastewater infrastructure from cyber attacks. Frontiers of Earth Science, 5(4).

Rao, V. M., & Francis, R. A. (2015). Critical review of cybersecurity protection procedures and practice in water distribution systems. IIE Annual Conference Proceedings, 2019-2028.

RISI Repository of Industrial Security Incidents. (2018) Water Sector Incidents. http://www.risidata.com/ (accessed April 2, 2018).

Rural Community Assistance Partnership. (2011a). A Drop of Knowledge: The Non-Operator’s Guide to Drinking Water Systems. National Environmental Services Center. https://rcap.org/wp-content/uploads/2011/12/Non-operators-Guide-to-DRINKING-WATER-Systems\_Small.pdf (accessed April 7, 2018).

Rural Community Assistance Partnership. (2011b). A Drop of Knowledge: The Non-Operator’s Guide to Wastewater Systems. National Environmental Services Center. https://rcap.org/wp-content/uploads/2016/01/RCAP-Non-operators-Guide-to-WASTEWATER-Systems.pdf (accessed April 7, 2018).

Santora, M., & Wilson, R. (2007). Water sector security and preparedness: A sustainable, all-hazards approach. American Water Works Association.Journal, 99(7), 33-34,36.

Sedlak, D. (2014). Water 4.0: the past, present, and future of the worlds most vital resource. New Haven: Yale University Press.

Shen, Lei. (2014). The NIST Cybersecurity Framework: Overview and Potential Impacts. Journal of Internet Law; New York Vol. 18, Iss. 6, 3-6.

Sorlini, S., Collivignarelli, M. C., Castagnola, F., Crotti, B. M., & Raboni, M. (2015). Methodological approach for the optimization of drinking water treatment plants' operation: A case study. Water Science and Technology, 71(4), 597-604.

Taormina, R., Galelli, S., Tippenhauer, N., Ostfeld, A., & Salomons, E. (2017). Assessing the Effect of Cyber-Physical Attacks on Water Distribution Systems. World Environmental and Water Resources Congress 2017.

Willis, Henry H., Anu Narayanan, Jordan R. Fischbach, Edmundo Molina-Perez, Chuck Stelzner, Kathleen Loa, and Lauren Kendrick. (2016). Current and Future Exposure of Infrastructure in the United States to Natural Hazards. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research\_reports/RR1453.html. (accessed April 5, 2018).