AUSTRALIAN WATER ASSOCIATION

water e-journal

ISSN 2206-1991
Volume 9 No 2 2023
doi.org/10.21139/wej.2023.004

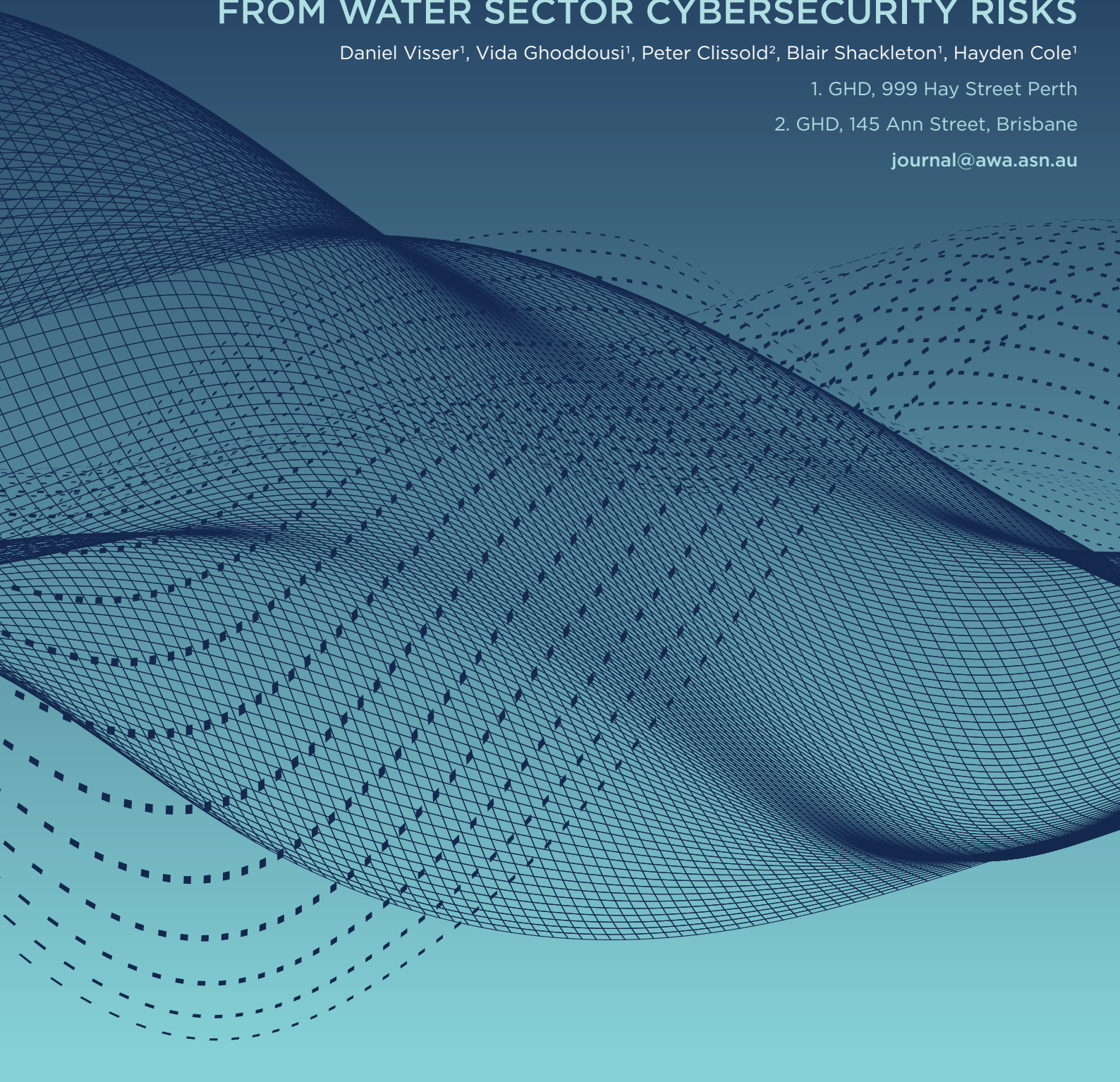
BEYOND DIGITAL: PROTECTING PUBLIC HEALTH FROM WATER SECTOR CYBERSECURITY RISKS

Daniel Visser[1], Vida Ghoddousi[1], Peter Clissold[2], Blair Shackleton[1], Hayden Cole[1]

1. GHD, 999 Hay Street Perth

2. GHD, 145 Ann Street, Brisbane

journal@awa.asn.au



AUSTRALIAN WATER ASSOCIATION
water e-journal
OPERATIONS

ISSN 2206-1991
Volume 9 No 2 2023
doi.org/10.21139/wej.2023.004

Beyond digital: Protecting public health from water sector cybersecurity risks

Daniel Visser[1], Vida Ghoddousi[1], Peter Clissold[2], Blair Shackleton[1], Hayden Cole[1]

1. GHD, 999 Hay Street Perth 2. GHD, 145 Ann Street, Brisbane

ABSTRACT

Historically, the design of water treatment plants relied on infrastructure such as pipelines, tanks and sand filters. Today the industry uses more advanced equipment, control systems, instrumentation and communication technologies. Improved technology brings benefits, but it also introduces cybersecurity risks. Due to the potential impact on public health, the potential for cyber attack on a water treatment facility is not an insignificant issue.

Are digital controls sufficient, or should additional methods be used to secure drinking water supplies? In light of the safety hierarchy of controls and the multiple barrier (Defence-in-Depth) approach, the authors contend that water authorities should be doing more to address the risk of cybersecurity events to water infrastructure.

Discussion about some opportunities to further reduce cyber risks is included in this paper. However, by no means should these considerations be taken as exhaustive. Cybersecurity incidents are a continuously evolving concern for most industries. Safety and security management must evolve faster to close the current gaps and keep pace with emerging risks.

INTRODUCTION

Over 100 years ago, by comparing the location of water resources and the prevalence of illness in the community, the late Professor John Snow demonstrated a clear link between public health and the quality of drinking water. Clearly, drinking water is essential for all aspects of life. Therefore, from a duty of care perspective, every effort must be taken to always ensure that water authorities provide consumers with water that is safe to use.
The Australian Drinking Water Guidelines (ADWG) are a nationally recognised document providing direction on the quality of drinking water to be supplied in all parts of Australia. They provide a risk-based framework for the good management of drinking water supplies.

A fundamental principle contained within the ADWG is that a drinking water system must have, and continuously maintain, robust multiple barriers to protect against potential contamination facing the water supply. This approach is universally recognised as foundational for safe drinking water systems. No single barrier is effective against contamination 100 per cent of the time, or constantly functions at maximum efficiency. Additionally, according to the ADWG, “a robust system must include mechanisms or “failsafes” to accommodate inevitable human errors without allowing major failures to occur.” By extension, it is evident that a robust system must also include mechanisms or “failsafes” to account for any risk of malicious action – through cyber attack or

otherwise.

Historically, the design of water supply and treatment systems relied upon hydrology and civil infrastructure such as pipelines, channels, pumps, tanks and sand filters. Many of the water industry's current assets are still built using a similar approach, with modern water assets designed, constructed and operated following sound engineering and maintenance practices. Furthermore, they are augmented with more technologically advanced pumps, valves, treatment modules, supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), and instrumentation. This augmentation provides the ability to optimise water management processes and more reliable access to safe drinking water. It also provides more timely responses in the event of water quality incidents.

The industry is characterised by a definite escalation in the use of computers, operational technology (OT), the Internet of Things (IoT) and machine learning. This means that modern water infrastructure has a much greater reliance on computerised control and is utterly dependent on them in many instances.

For example, networks of dams, pipes, pumps and water treatment plants are monitored and controlled by computerised systems providing real-time visibility of the health and status of the assets via SCADA systems. This has the added benefit that operators can monitor the plants from a remote office or even their homes with minimal interaction.

It is evident that SCADA systems and OT in general, significantly benefit the water industry. They improve plant operability, water quality and reliability through enhanced monitoring and control of assets. In addition, they provide a safer working environment for operators due to reduced travel requirements and in many cases elimination of exposure to hazards (such as chemical leaks, etc). However, the same systems that provide these benefits also introduce cybersecurity risks. It has been said that Smart Cities (and by extension "smart water supplies") are "cybersecurity war zones". If measures are not taken to prevent cybersecurity risks, the growth in automated water supplies will intensify the "battle".

WATER AUTHORITIES UNDER CYBER ATTACK

One author wrote "The prevailing feeling about why there has been so little focus on securing control systems is that it isn't real. What I constantly hear is "once there is a real control system cyber incident, I will spend the time and money to address the problem"." (Weiss, 2015)

Australian readers need only to reflect on recent cyber attacks on the Optus and Medibank facilities to recognise that the risk of cyber attack is real. Although the scope of this paper is not to study the intricacies of each event in detail, in the context of attacks made on the water treatment industry, the following publicly known examples could be studied:

- Israel 2020: cyber criminals affiliated with the Iranian regime attacked several facilities and attempted to increase the level of chlorine.
- Norway 2021: A ransomware attack resulted in the shutdown of water treatment facilities in 200 municipalities, affecting approximately 85% of Norwegians.

Multiple cyber attacks have occurred in the United States:

- Harrisburg, PA 2006: Hackers installed a virus on the laptop computer of an employee which could have altered the disinfectant levels in the potable water supply.
- Georgia USA, 2013: Perpetrators gained access to a water treatment plant control system and changed the fluoride and chlorine settings.
- Kemuri Water Company, USA, 2016: Hackers changed the levels of chemicals used to treat water during an attack on an outdated IT network.
- Ellsworth County, 2019: An offender gained access to the computer system and proceeded to shut down processes behind the facility's cleaning and disinfecting procedures.
- Oldsmar, Florida, 2021: An attacker remotely manipulated set points to increase the dosage of sodium hydroxide (caustic soda)
- San Francisco Bay, California, 2021: an attacker took control of a local water treatment facility and deleted computer programs.

Due to mandatory reporting laws, or the lack thereof, many more cyber attacks around the globe go unreported. To illustrate that Australian water authorities are not immune to cyber attack, the following examples are provided for consideration:

- Maroochy Shire, Sunshine Coast, Queensland, 2000: An attacker caused millions of litres of raw sewage to spill into local parks, rivers and a hotel.
- Victoria, 2020: Thousands of Victorians had their private details breached in a research bungle by three water companies.
- Queensland 2021: Cyber actors remained undetected in SunWater systems for nine months.

The auditors involved with the SunWater case revealed that cybersecurity (or lack thereof) is a widespread problem. The auditors examined the internal controls of six water authorities in Australia and found deficiencies in three, without naming them specifically.

CYBER ATTACK & PUBLIC HEALTH

Like many critical systems, modern water supply infrastructure relies on digital technology to keep high quality water flowing. Therefore, a system failure will impact the availability of services, which may have a cascade impact on the health and well-being of the community and the environment if not redressed promptly. More concerning, is deliberate misuse that can accelerate harm to a community.

Knowing the unknowns when addressing cybersecurity challenges in the water sector allows utilities and operators of critical water assets to plan for the inevitable cybersecurity event. We do not know where or when the next major cybersecurity event will hit, nor how vulnerabilities will be exploited to allow access to our OT systems. Therefore, we need to use what we know to help design resilience into our systems.

Plant assets and SCADA systems seldom hold information labelled as “Confidential”. However, the SCADA system itself contains a map of the process, and the process data provides insight into the dynamic nature of the water infrastructure. This information can give adversaries an advantage in understanding a system’s function and how to create the most disruptive impact on the environment.

Unauthorised use of the SCADA and ICS introduces the potential for maloperation of the system. This may lead to the interruption of water supply, or worse, compromising the safety of operators, the community or the environment. Such unauthorised behaviour may be the result of:

- A malicious intent
- Failure to follow defined change management and maintenance practices (taking shortcuts)
- Not realising what infrastructure is being controlled; and/or
- Not realising the consequences of adjusting settings.

The provision of a safe supply of drinking water is essential to the establishment and sustenance of communities. Without it, communities will not thrive. Inadequate water availability results in disruption and unrest. Unsuitable water quality can result in illness and/or community outrage. Unauthorised adjustment to water treatment system settings has the potential to result in:

1. Reduced water supply (flow):
   - Turning pumps off and potentially holding the controls for these at ransom: This may include disablement of potable water delivery pumps and/or raw water supply pumps such as bores. Either way, delivery of drinking water to the community may be impacted.
   - Operating valves such that flows are shut off or misdirected with similar consequences to the above-described disablement of pumps. The action of such adjustments on scour valves or similar may result in releases to the environment and wastage of water.

2. Impacts on water quality:
   - Operation of valves such that flows are shut off or misdirected; for example, unauthorised:
     - Shutoff of sludge extraction on a clarifier, resulting in rising sludge blanket levels and elevated turbidity, leading to overloading of the downstream filters.
     - Opening of filter bypass valves, resulting in the release of turbidity to the drinking water supply system, shielding pathogens from disinfection with UV or chlorine.
     - Opening of Reverse Osmosis bypass valves, leading to a release of raw water contaminants (not necessarily detectable using online instrumentation) such as

nitrate or arsenic.
- Closure of Reverse Osmosis blending bypass valves, leading to aggressive product water and corrosion.

- Operating plant incorrectly; for example, unauthorized:
  - Shutoff of filter cells such that feedwater is directed to fewer filters, leading to overloading of these filters.
  - Shut down of UV units, resulting in inadequate disinfection.
  - Disablement of filter cleaning/backwash operations
- Maloperation of chemical pumps; for example, unauthorised:
  - Underdosing of coagulants or flocculants, leading to elevated turbidity,
  - Overdosing of fluoride, leading to fluorosis risks, etc
  - Overdosing or underdosing of chlorine, resulting in unsafe disinfection practices.
  - Overdosing or underdosing of pH correction chemicals, impacting upon the aesthetics of the drinking water supplied, as well as the effectiveness of the disinfection methods.

Systems most at risk of impacts such as those described above are those where the product water from treatment plants is provided direct to the reticulation for customer consumption, without the opportunity for buffering in reservoirs or extensive pipe networks. However, this does not mean that systems having storages prior to delivery are immune to these risks. In the context of the principles applied by the ADWG, "dilution as a solution to pollution" is not a valid approach.

The risks resulting from the actions of cyber attackers have the potential to be made worse due to the potential of the perpetrators to:

- Mask indications, alarms and/or trends on screens to hide their activities.
- Alter or disable interface functionality, reducing the ability of operators to apply corrective action; and
- Alter stored data used for reporting, e.g. to the Department of Health.

In addition to direct impacts on public health as described above, the actions of cyber attackers may lead to damage to water treatment and/or supply infrastructure. Unauthorised operation of equipment, particularly pumps and valves can result in physical damage to plant and infrastructure; for example, unauthorised:

- Startup of Reverse Osmosis high pressure pump(s) with reject valve closed, leading to membrane damage.
- Hydraulic shock to UV systems, leading to lamp breakage.
- Shut down and restart of clarifier rakes, leading to over torque damage.

If a cyber attack does not result in material impacts to public health or damage to plant, it may still lead to non-compliance with the ADWG (water quality guideline exceedances or compromised reporting) and significant reputational damage to the organisation.

MODERN SCADA, CONTROL AND INSTRUMENTATION TECHNOLOGY

The industry has long relied on SCADA for the control and monitoring of plant and equipment, which often leverage infrastructure and technologies that are common to Information and Communications Technology (ICT) systems. However, the specific functions and priorities of SCADA systems mean their system requirements often differ from traditional ICT systems. When exploring the requirements of the application, building resilience into the network stack, and ensuring high availability for the computer platform, engineers quickly discover that the water sector requires many of the features and functions typically reserved for high end data centre, or critical network applications, only implemented at a much smaller scale. This often results in a skills gap between the system designers, implementers and support organisation.

The gap results in inadequate cybersecurity, and cybersecurity management practices, because the primary objective is to get the system working, with the focus on the SCADA, control systems and devices. It is important that when the system is designed, suitable experienced engineers are engaged to design and, where necessary, implement the specialised network and server capabilities.

The control system landscape has also evolved to include cybersecurity capabilities well beyond the simple use of access passwords. Critical systems

need to enforce access control but are also required to support the ability to control what actions an authorised user can perform, protect information in motion by using encryption for communications links, and implementing device integrity checking. While many applications do not require all these security features to be implemented, there are many systems being deployed in the water sector where cybersecurity risk assessments are finding that they are necessary to reduce the risks to a tolerable level.

Old school use of a firewall to protect the perimeter of the system is no longer sufficient to implement the whole of system cybersecurity protective controls. Firewalls still provide an important set of security services to support the segmentation and separation of critical and non-critical OT functions, and to isolate the OT from the IT domains, but they do not enforce, or provide many of the cybersecurity services required in the OT domain.

Compounding the need for additional cybersecurity services within the OT environment is the prolific use of computerised devices for instrumentation. Instrumentation is used in the drinking water industry to measure physical process variables such as temperature, pressure, pH, level, and flow. These measurements are used for local and remote indication via SCADA and serve as critical inputs in the control and/or monitoring of drinking water from catchment through to tap.

Instrumentation technology has evolved from mechanical and pneumatic devices such as gauges, turbines and Bourbon tubes to sophisticated electronic devices capable of performing complex calculations. Instruments which run software to perform calculations, self-calibrations, detect internal faults and communicate with remote devices, are considered 'smart' instruments. 'Smart' instruments offer additional information beyond the variable they measure. For example, a pH transmitter configured via a standard 4-20 mA interface will only provide information regarding pH. However, if it were connected as a 'Smart' instrument (via networks using protocols and standards such as HART or Profibus, etc.), diagnostics and data quality would also be available for remote viewing. 'Smart' instruments have the capability of built-in communications interfaces that allow more than the single variable to be communicated. They can perform internal calculations such as flow totalisation, for example, and these quantities can be directly interfaced with SCADA or other remote equipment.

Instruments and the data they provide are critical to the functions performed by a SCADA system. With the proliferation of network-connected instruments and smart starters, cybersecurity breaches present an ever-present risk which needs to be mitigated when considering the design, configuration management and maintenance of these devices.
Instruments with enhanced capability, or 'Smart' instruments, can provide detailed information, such as:

- Electronic calibration and configuration of parameters
- Measurement of multiple variables
- Data quality and diagnostics, including self-diagnostics
- Higher accuracies and resolution
- Time and date stamping

The use of smart instruments and digital communications assists water authorities to demonstrate compliance through remote online monitoring of the instrument, its calibration status and its health. This online monitoring is not possible without the use of smart instruments and digital communications. Therefore, secure communication networks are required.

Although the discussion herein has focused on the application of smart instrumentation, the risks described are not limited to these technologies. Many of the factors described (e.g. remote configuration) are also applicable to other smart devices (e.g. variable speed drives, smart starters) which present at least as much risk as smart instruments.

Operational Technology (OT) is currently less mature (relative to Information Technology (IT)) in its usage of ICT. While emerging technologies such as the Internet of Things (IoT) provide numerous benefits, it can make the OT systems increasingly vulnerable and increase opportunities for cyber attacks. A security breach can cost a corporation millions of dollars in contrast to the low-cost model offered by IoT, reinforcing the significance of cyber secure practices for critical assets. To ensure maximum resilience against cyber threats, digitally connected systems must be designed with security in mind (secure-by-design).

Lack of strategic oversight related to IoT adoption and cloud computing can potentially lead to increased risks associated with cybersecurity, breaches of data governance, breaches of standardisation policies and their enforcement, which in the long run, can present adverse impacts to the business. These risks need to be weighed up against the perceived improvements and benefits of the technologies being implemented.

Many OT systems were built and designed prior to the need for smart devices and IoT, which means they incorporate legacy technologies. In addition to their age disadvantage, they lack modern security controls, and security tools to provide adequate visibility into assets on the network. These systems are often fragile; a small change or abnormal activity within the network architecture can go undetected for a long time, and ultimately lead to costly downtime. For the water industry, even brief periods of downtime can have significant social implications. Water is fundamental to health and hygiene; critical system outages can impact the population's physical safety.

Water authority SCADA architecture should be scalable and flexible to support the business' functional, security, and corporate requirements.

CYBERSECURITY

Cybersecurity incidents can be broadly categorised into three key areas:

Information protection, commonly the domain of information security professionals, is where there is intrinsic value in the information being protected. For example, this could be trade secrets, personal information, financial details and health records. Protection of this information from loss or compromise is paramount.

Denial of Service protection (DoS) is the prevention of system loss, where real time access is required to maintain an acceptable level of service, maintain safety or supply. Typically implemented in the form of redundant capabilities, protection against DoS attacks minimises the downstream impact of a loss of function. Critical to the successful implementation of DoS protection, is the identification of single points of failure and eliminating them as much as possible. For example, a 2018 incident involving a water authority in North Carolina was a ransomware attack, locking systems and demanding a ransom for the return of operable systems.

Protection against deliberate attacks is the identification of actions that may compromise the operations of the asset, resulting in damage, harm or catastrophic failure due to the misuse of systems or equipment. The motivation of the threat actor in these cases may not be well understood, however, they are typically beyond the realm of financial gain, or incidental compromise. For example, the Maroochydore incident was, in part, motivated by discrediting the systems integrator, in an attempt to gain direct employment.

If we look at some of the historical events, we can also assign attributes to the different threat actors – insider, cyber-criminal, nation state or others. That, in some ways, talks to the motivation of a threat actor, and the level of cybersecurity controls required to protect against them.

The focus on cybersecurity by state and commonwealth governments has seen many water authorities attempt to tackle cybersecurity for their operational assets. Across the range of strategies, the overwhelming approach is to throw technology at an attempt to solve gaps in cybersecurity. After the obligatory cybersecurity assessment, the entity is left with a basket of problems that need to be addressed.

Assessments typically performed against the technical component of the standards, have outcomes that are aligned only to technology risks. The risk assessment generally has a limited scope, such as the OT systems, and specific sites or plant. This approach amplifies the focus on technology risks and lacks context of the organisation. As a result, cybersecurity risks tend to overstate the likelihood of a compromise, and often understate the real-world consequences.

Risks need to be identified and developed in the context of the organisation and the asset, and not be overly focused on the technology, to gain a full understanding of the risks from cybersecurity and the controls that need to be implemented to address these risks. Many organisations see this as a very big problem, and need to be seen to do something, but often this results in disproportionate response, costs, and effort.

To help address this challenge, organisations

look to implement cybersecurity management strategies aligned to the nature of their business. While there is a focus on information security for their enterprise environment, in many instances the enterprise would not exist without the operational technology. There are several cybersecurity management frameworks to choose from, however, there is one that is more prominent than others and includes specific elements to address OT systems. This is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is prepared and maintained by the US Government and provides an alternative to some of the commercially available standards. The NIST CSF is comprehensive, and continually maintained and enhanced to address emerging technologies. However, the NIST series of cybersecurity standards has a disadvantage in the ability to have cybersecurity management systems certified.

The NIST CSF lifecycle considers the following steps. Identify, Protect, Detect, Respond and Recover. Many of the organisations addressing cybersecurity predominately following the technical path, have ineffective cybersecurity management systems for OT. This is because, while the technical requirements have been identified, controls are implemented to protect and (in some instances) detect cybersecurity events. Seldom is sufficient effort spent in monitoring these systems, therefore, impacting the ability to respond and recover to indicators of compromise.

GOING THE EXTRA MILE

The cybersecurity events in the water treatment industry that are the most troubling are the insider events and nation state threat actors, who have a specific motivation to cause disruption or harm. In the case of nation states, it may be to establish persistence, to be exploited at a strategic moment, whereas for an insider, it may be to bypass security processes in an attempt to accelerate an activity, or a more sinister motive.
It is important to effectively manage this type of threat by implementing cybersecurity controls that allow the detection and treatment of indicators of compromise. The activities include the implementation of strong perimeter security, and secure remote access solutions from all networks outside of the OT environment. Security event notification and logging solutions, periodic scanning of the environment for vulnerabilities, implementation of application whitelisting, engaging people to review logs periodically, investigating unknown activities, tightening maintenance practices to ensure identification of known and unknown activities, and testing the performance of the cybersecurity controls will will lead to better detection and management of compromise.

The question is though: are digital controls such as those described above sufficient, or should water authorities be going beyond digital to secure water supplies? The authors contend that water authorities should be “going the extra mile” to ensure that risks are reduced to As Low As Reasonably Practicable (ALARP). The hierarchy of controls is a well-known and respected principle in the health and safety industry. In the context of this, authorities should aim to eliminate (or at least reduce) the risk of cybersecurity events. Furthermore, the ADWG promotes a multiple barrier approach. This principle applies no less to cybersecurity driven risks to water supply than it does to naturally occurring water quality risks. Discussion about some opportunities to reduce cyber risks is included below. However, by no means should these considerations be taken as exhaustive.

Many instruments (particularly water quality analysers) are provided for smart interfaces to the control system, potentially allowing recalibration, scaling, etc, from the control system. This is a significant risk for correct plant operation. Water authorities should consider options to limit risks of this nature. Clearly the first opportunity to do this is through appropriate selection of the specific analysers to be used and how they are to be configured. Particular care must be taken with final water quality (custody transfer) instruments.

The plant control system must remain subservient to local controls and display panels (not connected to external communications links) to ensure plant can at least be shut down safely in the event of significant maloperation. Shut-off valves on the plant outlet should facilitate isolation using local controls (disconnected from the control system).

For safety or public health critical processes, plant equipment should be designed such that it cannot be operated ‘dangerously’ (i.e. operated in a manner resulting in inappropriate water flow rates,

inadequate water quality or damage to plant. This could be limited by either physical constraints on the equipment (e.g. capacity of pump no greater than required, only physical [not remote] adjustment of pump capacity) or by hard wired limits (e.g. hard wired switch [flow, level, pressure, analysis]).

The above-described philosophy should extend to limiting operating sequences (e.g. a certain pump will not start until a specific valve is open, etc), being mindful that these interlocks should not be arranged in a manner that could ever be altered remotely through unauthorised access. Note:

(i) the industry is already routinely adopting this arrangement to prevent pumps operating with low water level in a tank.

(ii) this will require significant care in the functional design stage to ensure that plant flexibility is not unduly constrained.

Currently, there is a tendency for some water authorities and plant designers to add actuators and remote-control capabilities for most (or, in some cases, all) valves, because it can be done at low cost. In the context of cybersecurity, the wisdom of this choice must be questioned. At a minimum, the position of valves that do not need to be adjusted regularly, should be physically locked.

Fluoride dosing pumps and chlorination systems should have physical or hard-wired limits on their dose rates to limit the risk of overdosing into final product water. Other chemical dosing pumps should also be considered in a similar way, as they can also impact on water quality (i.e. coagulant dose rate, pH correction, etc). Designers should consider the inclusion of day tanks to monitor and limit the quantity of chemicals added to the water supply.

It is apparent from the discussion above, that much of the responsibility for mitigation of cybersecurity risks lies with the plant designer. The process of performing Hazard and Operability (HAZOP) studies, Control HAZOP (CHAZOP) studies, and Safety in Design, allows the designer to undertake an assessment of the hazards, risks and operability requirements. These processes should be used diligently and include consideration of cyber risks.
Mitigation of cybersecurity risks does not end during the design and construction phase. It must continue into operation. As an example, operators must ensure that they do not become accustomed to relying on SCADA as the only source of information. The importance of regular site inspections, visual observations and manual sampling should not be underestimated.

A novel approach to SCADA independent water quality monitoring is an approach used by the Israeli Eshkol water treatment facility in Beersheba, which utilises several fish aquariums in a manner much like the proverbial canary in the coal mine (Staff, 2020). Clearly, not all water authorities need to install aquariums. However, this example highlights the fact that innovation can reveal unique methods of risk mitigation.

It is essential that water authorities ensure that their operators have a comprehensive understanding of the plant(s) they operate. Operators should be trained to operate plants manually with a high level of confidence. This includes ensuring that operators know the characteristics of good/normal plant operation. For example, operators should know how often their plant is backwashed, how long it takes to empty a chemical tank and so on. Such knowledge is critical to ensuring that the operator recognises when a plant is behaving abnormally due to unauthorised remote access and allows appropriate responding action to occur. Knowledge should also be exercised periodically using mock incident drills to ensure that it remains current and accessible.

CONCLUSION

The water industry has made considerable inroads into the development of smart technologies that allow for fine tuning of plant monitoring and control. Whilst such advanced digital control systems provide convenience for operators, they also have the potential to introduce cybersecurity risks. It is critical that water authorities remain vigilant. Instrumentation, SCADA and IT systems must be designed with careful consideration for cybersecurity risks. However, this in itself is insufficient. In the context of traditional risk management approaches and the principles of the ADWG, designers, operators and maintainers must ensure that:

A) multiple barriers are in place (both electronic and physical) and

B) if a cybersecurity incident could occur, that the risks to public health are reduced to ALARP.

This paper has discussed several cybersecurity considerations, however, the content is by no means exhaustive. Cybersecurity incidents are a continuously evolving concern for the industry. Safety management must evolve at the same rate or (preferably) even faster.

THE AUTHORS

Daniel Visser is a Chartered Chemical Engineer and Chemist with specialist experience in water treatment and desalination. He has extensive experience with the Australian Drinking Water Guidelines (ADWG). His experience includes planning, tender design / evaluation, concept design / modelling, through to detailed design, construction / commissioning advice and troubleshooting.

Vida Ghoddousi is a principal instrumentation, control and SCADA engineer with over 30 years of experience. Her experience spans across the water, wastewater, power, mining and food industries. Vida has considerable experience in the water sector, including multiple project experiences on water treatment projects – both large and small.

Peter Clissold has more than 25 years of experience in industrial automation, SCADA and networking design and implementation. He has a unique combination of skills and experience across the water industry. Focused on helping operators, Peter identifies vulnerabilities and designs mitigation strategies and controls to reduce cyber risks within critical assets.

Blair Shackleton is a Chartered Chemist with over 35 years of experience in water. He has gained extensive water quality and treatment experience through numerous water treatment plants for water utilities, power utilities, mining and industrial companies. Blair has comprehensive knowledge of the principles of the Australian Drinking Water Guidelines (ADWG).

Hayden Cole has over 17 years' experience in industrial automation, control systems and information technology design and design management. He has extensive project experience designing and delivering automation projects in water, power and mining applications. He has considerable water experience across all asset types including large greenfield water treatment plants.

REFERENCES

Germano, JH., (2018) "Cybersecurity Risk & Responsibility in the Water Sector", American Water Works Association

Hassanzadeha, A., Rasekhb, A., Galellic, S., Aghashahid, M., Taorminae, R., Ostfeldf, A., Banks, MK., (2020) "A Review of Cybersecurity Incidents in the Water Sector" Journal of Environmental Engineering 146

Namdar, S., Karlsik, A., Smith, R., Price, G., McPhee, A., (2020) "Cybersecurity: A Foundational Requirement for a Modern Water Utility", Cisco/ Jacobs

NHMRC, Australian Drinking Water Guidelines 2011

Staff, T, (2020) https://www.timesofisrael.com/alongside-high-tech-systems-these-fish-stop-iran-hacking-israels-water-supply/ (accessed 31 October 2022)

Weiss, J.M, (2015) https://www.advisenltd.com/2015/07/30/lost-in-the-limitations-of-cyber-15b-in-control-system-losses/ (accessed 26 October 2022)