Questions and Answers from WaterISAC and EPA webinars, entitled *Cybersecurity Recommendations in Consideration of the CISA/FBI/NSA Advisory on Russian State-Sponsored Cyber Operations Against U.S. Critical Infrastructure* held on 12/29/2021 and 1/5/2022.

NOTE AND DISCLAIMER: These written responses to questions from webinar participants are being provided where questions could not be addressed during the webinar due to time limitations. The responses to the questions below reflect the views of individual webinar presenters and not necessarily the positions of WaterISAC or the USEPA. All recommendations are nonbinding suggestions unless otherwise stated and may not apply in all situations. The naming of specific products or services does not constitute endorsement or preference versus competing products or services.

12/29/2021 Webinar

What level of skill set, fulltime internal resources do you recommend? Also, should you recommend backup of those skill sets as well? [utility superintendent]

> The resources that a water or wastewater system can apply to cybersecurity will vary depending on factors like the number of customers, rate base, and competing resource demands, such as asset management and regulatory compliance. All water and wastewater systems, however, should conduct an assessment for cybersecurity vulnerabilities and establish a prioritized list of actions that the utility can carry out with available resource to mitigate the most significant vulnerabilities.
>
> Where possible, having two full-time cybersecurity staff is beneficial. Multiple cybersecurity staff can support each other with technical issues, split on-call coverage and schedule vacations at different times. Ideally, they should report to someone that reports to the CEO or to the Board. In addition to the two people solely focused on cybersecurity, regular IT and OT operators should take a mix of technical cybersecurity classes. Having technically knowledgeable cybersecurity staff in both IT and OT domains will help advance the cyber maturity of your organization. It will also provide a feeder path if you lose a full-time person.
>
> Have a monthly meeting to review cybersecurity goals and progress with an organizational leader who has a technical role with cybersecurity or has a vested interest in success. There is also the value of cybersecurity awareness training across the organization, with an extra emphasis on anyone with an administrator account, in a manager's role, or in a process control role. In terms of a skill set, hire the two suggested full-time staff with as much experience as possible, including an educational background and field experience in cybersecurity. Novices can be supported by more experienced contractors until they get their footing.

Could a WARN be a good partnership to keep a specialized IT/OT firm on retainer for access to all members? [water association person]

> Cost sharing among water systems for external IT/OT support could be a means for specialized expertise to be available to a larger number of utilities. Whether this cost sharing was executed through a WARN or a different vehicle would be determined by the participating utilities.

Any specific examples of Spearphising used for this? I have seen a bit of Spearphising, but I was wondering about Spearphising specifically related to targeting water and waste water systems individuals. [municipal IT security person]

> Water utilities are subject to the full panoply of common spear-phishing tactics that are used against other businesses, such as spoofed emails targeting administrative and IT/OT personnel. One Spearphising email that was the initial step of a successful ransomware attack against a water utility in 2021, contained the utility's own prior correspondence with an engineering firm that was taken when the adversary breached the engineering firm's email system. The phishing email contained an encrypted DocuSign document with a malicious macro.

Andrew, are you recommending any iOS app (iPhone) to store passwords? [state primacy agency engineer]

> Unfortunately, we are not in a position to recommend products, but I think a regularly patched and conservatively used iPhone is a good platform for securely maintaining a password manager. Beyond having a strong master password (18+ characters) for the password manager and turning off automated password autofill, if that is on by default, I would suggest looking for the following product features:
>
> 1. The encrypted password data can be stored locally on the iPhone without having to put it in the cloud. *(This means you will not be able to sync it between various devices. It also means that your data is not in a cloud system that could be wholesale-targeted by an advanced adversary.)*
> 2. You can make local backups of the encrypted password data via iTunes to an external encrypted storage device. *(Making regular local backups is an essential step when you keep the data only on your phone.)*
> 3. Go with one of the well know and well-reviewed password managers that have been around for a while. *(Presumably they are better resourced to keep up with security issues and outside people have had a change to bang against those products for a longer time.)*
> 4. I would lean towards password manager products with slower hashing algorithms, which helps protect against brute force attacks if someone selects a poor master password. One way to find out the relative speed of some products is to look at the benchmark cracking specs for hashcat using a graphics processor (e.g. search on "hashcat RTX 3080 benchmark github"). They seem to be in the thousands (K) or millions (M) hashes per second, which is much slower and better than a standard Windows PC hash rate in the low billions per second.

Assuming there is adequate separation between process system and business network, how many of these could affect the process control system? [consultant]

> "Adequate separation" between IT and OT can mean different things to different utilities. Examples of separation architecture, in order of increasing stringency are using: 1) VLANS, 2) a router, 3) a firewall, 4) a pair of firewalls from different manufacturers, 5) a data diode, and 6) no physical connection at all. Also affecting the answer is what sort of traffic is passing over the architecture. That could include things like: internet traffic, email, active directory authentication, "outbound" process data collection, and viewing, maintaining or operating the water/wastewater control system. Finally, there may be good separation between IT and OT, but remote access exists from the internet to the OT system.
>
> In general, many of the vulnerabilities exploited by the Russian state-actors exist with separation architectures that depend on VLANS, routers, or firewall(s), with variations depending on the type of data transfer normally going on. Once you shift to data diodes with traffic only moving from OT to IT systems or true separation without any connections, you shrink the immediate vulnerable list down to supply chain issues and USB malware designed for air-gapped systems. Both of these techniques are in use by APT groups and criminal enterprises. Once in a control system, an automated program can take advantage of other vulnerabilities.

Are there any publicly (or privately) curated lists of common SCADA malware payloads or snort/yara rules that we could look to apply to our IDS/IPS? This may fall under patching/mitigation, but operating systems updates tend to be a big issue - a lot of our SCADA software is not compatible with newer OSes and as such, the latest and safest versions of various software are not available. So this is kind of patching, but also.. the patches are available, but we can't get to them. Can you provide a direct link to the EPA cybersecurity assessment program? [regional cybersecurity person]

> We are not aware of maintained repository of YARA rules for SCADA malware. You are probably aware that CISA frequently provides YARA rules with their ICS-Alerts. Older SCADA software compatibility with newer OSs is a problem that is hard to get around without expensive upgrades. Here is the link to register for the EPA cybersecurity assessment program: https://horsleywitten.com/cybersecurityutilities/

Some OT devices do not allow for these actions. [utility technical manager]

> That is a good point. OT devices and software often do not have security options such as multi-factor authentication capability. In the short term, try to implement compensating controls that help address the vulnerabilities you have identified. For example, messaging to your controller might not be secured using public key infrastructure authentication. In that case, you could implement a firewall between your HMIs and controllers that lets you provide some communication source protection, or you could implement a Host Identify Protocol system to more strictly define what device can talk to what device. In the long term, plan on capital improvements to upgrade your systems.

1/5/2022 Webinar

Airgap...wasn't the Natanz facility in Iran "airgapped" when they were hit by Stuxnet? [Wastewater management]

> Correct. That speaks to the risks that “air-gapped” systems face from supply chain issues, vendor laptops, insider threats, USB based malware, etc. USB based malware is used by both state actors and criminals. It is commonly used for espionage purposes but can be adapted for disruptive or destructive purposes against a water utility.

Can you speak at all to the intersection between water/wastewater utilities and electrical utilities? Given that several of the previous attacks targeted (Ukrainian) electric utilities, what response plans should water operators put in place for extended electrical outages? [System committee person]

> All water and wastewater systems should prepare for power outages regardless of the cause. EPA provides valuable information on increasing power resilience at water utilities, including backup power generation and incident action checklists for power outages, here:
>
> https://www.epa.gov/communitywaterresilience/increase-power-resilience-your-water-utility

How do you feel about granting contractors access to your DCS through the internet" [Utility technical person]

> It is not ideal, but it is a frequent necessity. Where it cannot be helped, make sure the vendor can only gain access via a jump box in your DCS’s DMZ that requires multi-factor authentication. Remember that the security of the approach depends on you staying on top of the software patches and firmware updates required for the equipment and programs you used for the remote connections. The security of the remote access is only as good as the security of the contractor’s remote computer and network. If that is compromised, there is a potential for your system being compromised. If you have a 24/7 operations center, leave the remote connection for the contractor normally disconnected. Connect it only when the contractor needs to do work and disconnect it afterwards. Even if you do not have a 24/7 operations center, consider following this connect-as-need tactic depending on the services that you need.
>
> If you can afford it, a better approach would be to pay the extra cost for the contractor to travel to your site to do the work. If you follow that path, require them to use your utility’s clean single-purpose laptop and other utility owned network equipment to do their work to avoid cross contamination from anything tainted by their working at a previous facility.

Does WaterISAC have a suggested training course for critical infrastructure employees? [Utility manager]

> The DHS CISA National Initiative for Cybersecurity Careers and Studies (NICCS) provides a wide range of free cybersecurity training resources (https://niccs.cisa.gov/training). In addition, the Idaho National Laboratory offers free training in ICS cybersecurity. Courses range from excellent introductory on-line classes up to an advanced week-long red team – blue team training session in Idaho. You can find more information at: https://inl.gov/critical-infrastructure-protection-training/

Is "air gap" a valid cyber security strategy? [Utility manager]

> Establishing an “air gap” by having no network connections or by using a data diode connection is a valid cyber security strategy. It is a strong perimeter defense that eliminates a number of risks and vulnerabilities that an adversary might take advantage of. However, it leaves plenty of serious supply chain, vendor laptop, “sneaker net”, and insider threat risks that still need to be mitigated.

Are there any funding provided by the government to help with financing [Utility technician]

> Funding for cybersecurity projects is available through both the Drinking Water State Revolving Fund (DWSRF) and Clean Water State Revolving Fund (CWSRF) programs as managed by the states. Guidance on the eligibility of cybersecurity projects is provided on these EPA fact sheets:
>
> - Drinking Water: https://www.epa.gov/sites/default/files/2019-10/documents/cybersecurity_fact_sheet_final.pdf
> - Clean Water: https://www.epa.gov/sites/default/files/2021-05/documents/cwsrf_cybersecurity_fs_final_0.pdf
>
> Contact information for state level SRF programs is available from the EPA at these sites:
> - Drinking Water: https://www.epa.gov/dwsrf/state-dwsrf-website-and-contacts
> - Clean Water: https://www.epa.gov/cwsrf/state-cwsrf-program-contacts

UPS should be designed to allow for alerts and data backups. [service provider]

> Uninterruptible Power Supplies (UPSs) are an important tool in providing clean and continuous energy to OT and IT equipment. If you set up UPS alerts, be careful how you do it. There is a certain amount of risk created if you communicate with your UPSs on a network that an adversary might be able to gain access to. That may let them selectively disrupt power to your IT or OT equipment.

Even scarier than USB keys are chargers that have malicious code in them. (Hence data blockers.) [System committee person]

> There are several generic looking products that you would expect to do one thing but are designed maliciously to do another. One example is a charger with a USB port that can inject malicious code. Others have included an AC power strip packed with surreptitious communications gear and a USB cable that can provide WiFi access and inject keystrokes payloads. This represents one aspect of supply chain risks. The lesson for us is to know where our products come from and what we have connected to our systems.