Case study report

Aiden Hetherington 102565475
Ekrar Uddin Mohammed Efaz 103494172
Joel Boatman 102091019

Organisation: Natanz uranium enrichment plant

Executive summary

This paper focuses on the Multi-layers of protection, from physical parameters to network security controls, should be deployed as part of a defense in depth (DID) strategy for the security of Industrial Control Systems. IDS and IPS, which use strict firewall policies to protect and segment assets across ICS/OT and Enterprise IT networks to create a "air-gapped" architecture. To manage the risk of obsolete assets and provide monitoring in detecting illegal or misused activities, audits and frequent patch management should be conducted in conjunction with these controls. Development, Implementation and Monitoring of a personnel awareness training program is suggested to lessen the risk of insider threats. Finally, application and device whitelisting has been adopted to provide security against spread of malware through removable devices.

Introduction

The Stuxnet worm Is believed to be one of the most dangerous worms that is currently known in the IT industry, largely due to the fact that it was highly targeted towards the organisation’s assets and utilized multiple layers of attack using multiple zero-day attacks and using multiple rootkits to stay hidden. It also helped open eyes to malware that was able to infect Industrial Control Systems (ICS), and in the case of Stuxnet, able to infect ICS when they are separated from the network [1].

The purpose of the Stuxnet worm, although still somewhat disputed, is largely said to have targeted the programmable logic controllers (PLCSs) that controlled the centrifuges in the nuclear plant. The aim was to temporarily adjust the speeds/frequencies of the centrifuges without it being obvious to wear them down and destroy them [2]. To do this, Stuxnet utilized 4 zero-day exploits, multiple rootkits to hide itself from intrusion detection and was able to self-update with an internet connection. It is assumed that the Stuxnet worm was originally introduced on a USB drive. The worm was able to travel over the network to infect other windows computers searching for the specific PLC software that it can infect [3]. If the software cannot be found, the worm will stay dormant on the computer and keep spreading to any new computers it can find. Once it has infected a computer that contains the PLC software, in this case SCADA systems, Stuxnet is able to modify the DLLs containing the code meant for the ICS and inject its own instructions. The injected code took a snapshot of the ‘working’ system that it could read while running its altered code, hiding any discrepancies from appearing and making the system seem as though it was working normally [4].

Stuxnet is also able to attach itself to any removable drives that are plugged into an infected computer and use the USB to bridge any air gaps. In the case of Stuxnet, when users plugged in a USB to transfer the real data to the ICS the worm will also attach itself to the drive and go to wherever it is then plugged in.

Although the Stuxnet worm is the most prominent and well-known worm that affects ICS there have been multiple others that have been introduced and caused large amounts of damage. There have been attacks on power grids that have taken out the power for large areas [5] as well as attacks on safety systems that could have the potential of taking lives [6].

Risk analysis

In order to construct security policies for the relevant organisation, a risk analysis is performed firstly by identifying assets and their values in terms of the cost to acquire, maintain and protect, the price others are willing to pay to destroy and the cost to have that asset replaced. Once these assets have been prioritized, the vulnerabilities and threats associated with each asset are determined and given scenarios describing each possible significant threat and outcome per the Delphi method. Possible countermeasures are also detailed, so a cost/benefit comparison can be made to analyse if the cost is appropriate to the effectiveness of the countermeasure. Obtaining a risk value is based on the probability of the threat to occur and its impact on the organization by using an integer range from 1 to 5, we can multiply these values to obtain a risk value out of 25. The same will be done in finding the effectiveness of the countermeasure.

Organisational assets:

- PLC
- Windows PCs
- USB flash drive
- ICS Physical Components
- Personnel Safety Equipments

Threat: Malicious/unintentional insider introduce the spread of malware.

Assets: Windows PCs, USB flash drive.

- An all too common vector of attack in ICS is the negligence of insiders where personnel create vulnerabilities via their actions. An example of such a threat event is the introduction of the spread of malware via USB drive, from which an inside actor is either oblivious to security standards and guidelines or is a disgruntled employee with malicious intent seeking a form of revenge. However, from the perspective of a uranium enrichment plant, it is a state-sponsored attack driven by political intent that can prove to be the most damaging as was the case of the Stuxnet malware in 2010. A preventative measure these industrial organisations should adopt is a strong personnel security policy that defines security awareness and training. The effective cost of this solution depends on the time spent implementing the program and the level of knowledge of employees and the procurement of learning materials which can vary.

Threat: Altering ICS via Malicious Program attached to Removable Media

Assets: ICS, PLC, ICS software, PCs

- It is assumed that the Stuxnet virus was introduced in exactly this way, attached to a USB drive that was inserted into a computer and then travelled from there through the network and attached to other removable devices. To prevent a similar attack whitelisting will be a great preventative method. Application whitelisting will make sure that only known applications can run and will remove the ability of malicious programs running. Removable Device whitelisting will also be

used as it will ensure that only verified devices can be inserted and used on computers. Both methods are low cost as they can be set up on an existing Windows Server domain. The only cost would be for antivirus software as some of it has Device control as an optionally add on.

Threat: Using Backdoor access to leverage control over ICS equipment.
Assets: ICS, Administrator Computers, Business Network

Backdoor ICS threats are a real concern following Stuxnet. Since a backdoor takes command from a C2 server and gives the attackers full control of the system in case of ICS they have full control over the physical components of the Industrial plant including the safety systems which gives the attackers immense power to harm. In a nutshell, if an attacker logs into an ICS system as if he were the user (Privilege level of such backdoors varies and that depends on the level of privilege escalation the attacker can reach.). After infecting the system, the RAT will establish a command and control (C2) channel with the attacker's server, through which commands and data can be sent to the RAT. RATs typically include a set of built-in commands as well as methods for concealing their C2 traffic. RATs can be bundled with extra functionality or designed in a modular fashion to provide extra capabilities as needed.

Delphi Method risk assessment

Threat	severity	likelihood	Effectiveness of countermeasure	Relative cost of countermeasure(1 is most)
Altering ICS via Malicious Program attached to Removable Media	5	1	3	5
Remote control over infected device via backdoor	5	2	4	3
Malicious/unintentional insider introduces the spread of malware	4	2	3	2

Security programme

Threat – Altering ICS via Malicious Program attached to Removable Media

Policy – Application and Removable Device Whitelisting for approved Programs and Devices

Standards:
- All applications and Removable devices Blocked
- Whitelist only the applications that are necessary to run
- Whitelist only the Removable Media (mainly USBs) that are completely necessary. These devices should only be with trained professionals. (See Personnel Policy)

Guidelines:

- IT Specialist must be contacted if a new application is needed or if a new USB device is going to be used

- Removable Media should not be taken off site unless completely necessary.

Threat: Malicious/unintentional insider introduces the spread of malware.
Policy: Personnel to undertake a continuous Security Awareness and training program

Standards:

- Assess and prioritize the security awareness needs
- Assign roles and communicate the need for the program
- Establish a bar relating to competencies that employees need to grasp.
- Personnel need to be aware of the threats that pose a risk to assets and the countermeasures to oppose these risks in relation to established policies.

Guidelines:

- New staff are required to undertake the security awareness program and review within 30 days of their hire.
- Existing employees will undertake this program in a quarterly manner to retain information.
- Third-party contractors and vendors who require access to critical components need to be carefully evaluated based on their knowledge, skills, and abilities (KSAs) and need to undertake a short awareness program before access is granted.

Threat: Using Backdoor access to leverage control over ICS equipment and computers.
Policy: Strict restrictions on systems with scheduled essential patches.

Standards:

- Regular Patch Management
- System audits for security
- Strict firewall policies

Guidelines:

- Using Decision tree "ICS-Patch" to ensure the most essential patches are applied urgently.
- Keeping low-threat patches in queue to make sure important patches are not delayed.
- Regular and strict system audits to check for malicious or unintended changes made to the system.
- Strict process monitoring to make sure only the necessary processes are running.
- Firewall policies to segment the business network and the site network.
- Monitoring all the outgoing traffic from the site network.
- Implementing IPS and IDS to reject any connection evading the firewall.

Implementation of security programme

1. Security Measure for "Backdoor" threat

1.1. Regular Patch Management

Applying security patches is a component of a cybersecurity programme, which is part of a risk management programme. An organization's goal is not to have fully patched cyber assets.

Its purpose is to keep risk to an acceptable level. When security patches are the most efficient and effective way to reduce risk to an acceptable level, they should be applied. The ICS-Patch project was created to help ICS asset owners decide what to patch and when [7]. The ICS-Patch project was suggested by the Founder of S4 Events "Dale Peterson" who is a huge contributor in the ICS security community.

Two main objectives:
1. To decide what to patch when in an asset owner's ICS based on the contribution of each security patch to risk reduction.
2. To automate the decision-making process for what to patch when, so that no human interaction is required after the ICS-Patch process is configured to provide the recommended patching decision for each available security patch.

When compared to the typical enterprise cyber asset and enterprise network, most ICS cyber assets and the ICS itself are static, rarely changing. This enables most of the decision points to be static and drawn from the asset inventory.

We could use the ICS-Patch decision tree to run updates by ranking the urgency of the update based on decision points. It can be looked at like "what to patch when". The decision tree ends in three results:

- Defer: Manual activation required.
- Scheduled: Schedule the patch to be applied at the next window.
- Urgent: Apply patch on the asset as soon as possible.

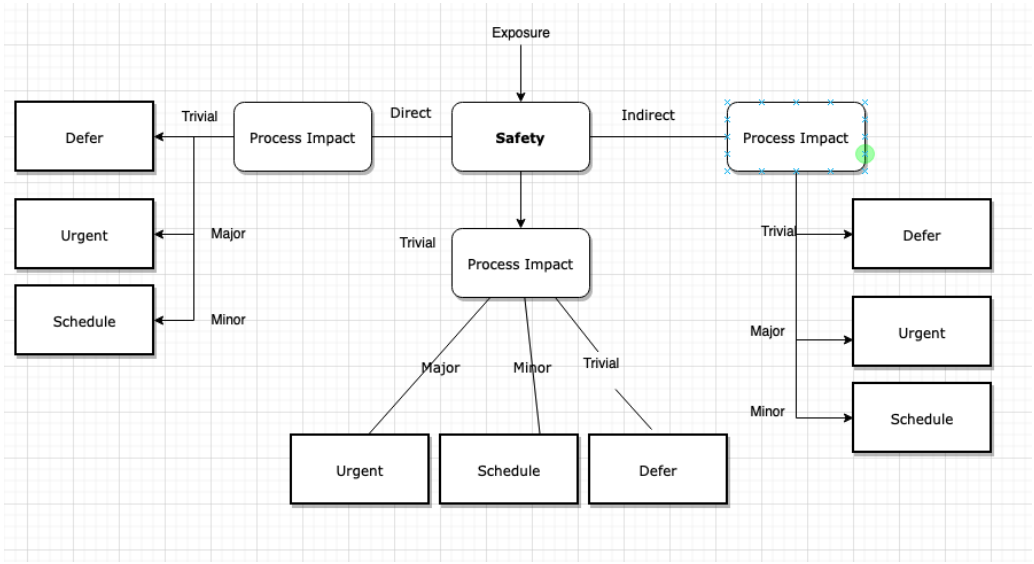
Decision Points

- Exposure: The first decision point in the decision tree is the vulnerability of the ICS cyber asset to attacks. If an attacker finds it extremely difficult to gain access to the cyber asset, it can be deferred (not ignored) in contrast if the vulnerability gives access to privileged zones, then more appropriate to apply patch ASAP.
    - Direct: Exposes the asset directly to attackers.
    - Indirect: Exposes other low value asset to attackers which might lead to high value assets upon further exploitation.

  Safety Impact:
    - Direct: If abused, the vulnerability would allow an attacker to change or disable safety safeguards, rendering them ineffective. Thus, directly impacting the safety of human lives.
    - Indirect: If exploited, the vulnerability has no direct impact on the safety of the process being monitored and controlled. To have an effect on process safety, the attack would need to compromise additional systems.
- *Process Impact*
    - Trivial: Little to no impact on essential services.
    - Minor: Activities that directly support key activities are harmed or disabled, but the process can still work for a while.

- Major: When activities that directly support vital processes are unavailable, the process ceases to function properly.

Decision Tree



1.2. System Audits for security

Data on the use of system resources is collected during auditing. The audit data keeps track of system events that are linked to security. This information can then be utilised to assign blame for actions that occur on a host on the contrary it can also be used to detect suspicious activity from a malevolent user hiding in plain sight. Identification and authentication are the foundations of successful auditing.

The audit service allows for the following [8]

- Surveillance of security-relevant events on the host and recording them in a network-wide audit trail
- Detecting illegal or misused activity
- Examining access patterns and persons' and items' access histories
- Discovering attempts to bypass the protection mechanisms
- When a user changes identities, they may discover extended use of privilege.

Security Audit Checklist

- Analyze security patches to ensure everything is up to date.
- Monitor attempted security bypass attempts.
- Monitor access to sensitive information objects in the organization.
- Monitor inactive accounts and attempt to remove/restrict them.
- Ensure zero trust and least privilege policy is implemented.

System Administrator Responsibilites

Monitoring Processes in Linux and scheduling regular tasks using cron.
Monitor Windows Processes to look for unscheduled activity.
Use of ADDS Software Restriction Policies to create highly restricted configuration of computers

Audit timelines depend on the type of organization that we are dealing with. In case of ICS two types of security auditing would be the best practice. They are:

a. *Routine Audits*

Routine Audits are done periodically to ensure a scan of the organization relevant systems to detect any suspicious activities or unusual resource usage. All the security perimeter bypass attempts, and secure object access are to be monitored as well to detect any backdoor access attempts made. Routine audits are usually performed by System Admins of the Organization

b. *Event Based Audits*

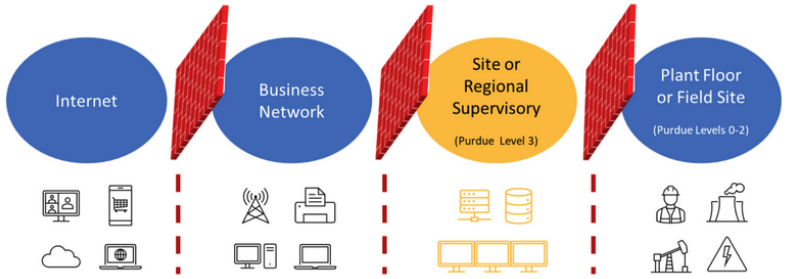
In the event of an attack, such as a data breach, the audit will concentrate on determining exactly what occurred and what went wrong to allow the leak to occur. Further audits should be done post-attack to detect any backdoor/RAT installed by the attackers.
Moreover, organization IT environment will be drastically different from when the last audit was completed after a big update, such as the installation of a new tool or a data migration.
An audit is a precaution against new vulnerabilities that may have been introduced because of the large-scale modification in this situation.

Given the time and resources required for a thorough security audit, it's critical to identify the level of effect of a change that would trigger an audit.
This prioritising guarantees that security team's resources are allocated wisely.

1.1.Strict Firewall Policies

Separating the ICS network from the corporate network is usually advised when building a network architecture for an ICS implementation. On these two networks, the nature of network traffic differs: On the corporate network, Internet access, FTP, e-mail, and remote access are often permitted, but not on the ICS network. The suggested network segmentation is a simplified form of the Purdue Reference Model introduced by Purdue University in the early 90’s for better network security of ICS. The goal of the model was to define best practices for the relationship between industrial control systems and its relevant business networks [9].

The organization has a lot of divisions that are interconnected for the smooth operation of the plant. There should be a firewall segmenting each division from the other and strict monitoring should be implemented. Key aspect of the network design should be to segment the ICS/OT and Enterprise IT networks such that an “airgap” architecture ensures there are no direct interconnections between the two. The administrators have to setup Firewalls that carefully monitor access with demilitarised zones (DMZs) have been used to connect these two levels. All connection between IT and OT is mediated via firewalls, with the purpose of eliminating direct communication between the two areas.



Firewall Policy checklist

- firewall should block all communication in and out of the ICS network and explicitly permit only the minimum required communication.
- To move files into and out of the ICS network while scanning for malware, a secure mechanism should be provided.
- Additional layers of verification, including multi-factor authentication, should be required for all access to the ICS network.
- Internet should not be accessible by the ICS network.
- Implementation of IPS and IDS to catch anyone bypassing firewall policies.

Application and Removable Device Whitelisting for approved Programs and Devices -Implementation:

Application Whitelist

For both whitelisting implementations we are assuming that the end user is using a windows server-based environment with all the networked computers on the same domain. First of all, we will look at how the application whitelist can be implemented. As whitelisting suggests, all of the applications will be blocked on the computers with only the applications/programs necessary for business allowed to run. A few best practices should be followed to make sure everything continues running smoothly with little to no downtime whilst the policy is being implemented:

- Before any of the technical procedures are followed a list of all of the important programs should be sourced as to limit any unnecessary downtime caused by necessary programs being blocked

- Before rolling out the policy a testing phase should be undertaken where a test device is set up with the restrictions and relevant tests are run to make sure only allowed software can run [10]

- When deploying the policy to users only a few selected devices should be set up, deploying in stages. This way if there are any issues with the restrictions there is a much smaller group who are affected meaning less downtime during implementation[10].

As we are assuming that the computers are on a domain the best way to configure the application whitelist would be through a software restriction policy that is deployed by group policy. When designing the implementation, it should only be the 'at risk' computers, or those directly dealing with the software that communicates with the ICS, that the applications are run on. For this it would be best practice to put those devices into their own organisational unit that can be assigned a group policy, this will minimise unnecessary management that could become increasingly tedious as more and more computers are needing to be managed.

Procedure:

1. Ensure all of the computers have been moved into their own OU
2. In group Policy management select the OU and create and link a GPO here
3. Select edit on the GPO and under the user config go to Policies, then Windows Settings, then Software restriction settings, right click it and create a new software restriction policy.
4. In the enforcement window make sure all software files and All users are selected.
5. Set the security Level as disallowed
6. Under additional rules add the paths for all of the software that the devices should be able to run making sure they are all set to unrestricted.

Removable Device Whitelist

There are two ways that the Removable Device whitelisting can occur, for the computers connected to the network they can be set up using group policy similar to the application whitelisting however for the devices that are not connected to the network or internet it will need to be set up using antivirus that allows the removable device whitelist feature.

As discussed with the application whitelist a testing phase should be run prior to official implementation to avoid any downtime due to improper setup. The rollout should then be done in section to ensure there is not a backlog of unknown devices that need to be added into the system [10] however where possible a new batch of removable devices should be sourced and used as opposed to reusing current devices to minimise the spread of any potential malware already on existing devices.

Procedure:

1. Get the device IDs of all removable devices that are going to be used

2. In Group Policy Management create a new policy for the whole domain and select edit

3. Browse to computer config, admin templates, system, device installation, device installation restrictions and enable "Allow installation of devices that match any of these device IDs [11]

4. Here all the Device IDs that were gathered earlier can be entered

5. Once all the devices have been added enable the "prevent installation of devices not described by other policy settings" policy.

6. Once these two are done only the devices that are specified by their IDs should be able to connect to the computers

Antivirus for Whitelisting

Some of the computers are separated by air gaps and are not connected to the internet or network at all. In order to protect these with whitelist in a similar matter to those networked computers an antivirus software with whitelisting capabilities is needed. Within the antivirus software it should allow for explicit rules to be added for what software is able to be run, similar to how it was deployed in the group policy. Devices plugged in should also be able to be manually added through the antivirus leaving any unrecognised devices unable to work.

This feature should be present with most antivirus solutions however may come as an extra cost that will need to be added on top.

Making sure these are all in place should minimise the chances that any code brought in on malicious devices will be able to run or affect any of the vital ICS.

3. Personnel to undertake a continuous Security Awareness and training program

The organisation shall design, develop, implement and monitor a security awareness and training program. Following this program staff will be given security awareness and training materials before they are permitted access to their relevant systems. To ensure this any personnel training needs to be documented and monitored.

3.1 Designing an awareness training program

An awareness and training program will be developed using a Fully Decentralized Program Management Model-based on NIST Special Publication, no. 800-82 recommendations.
In this model, a CIO/IT security program manager spreads policy and expectations regarding security awareness training requirements. Sub organisational units are used to carry out needs assessments, budgets, training plans and the implementation of the program. This has the benefit of dealing with units that have been segmented due to the role and security requirements applied in the defence-in-depth approach [12].

3.1.1 Needs Assessment

Once organisational units have been identified, a ‘needs assessment’ based on these distinct units is to be completed to determine the awareness training needs of personnel. Carried out by personnel from executive management to system users’, methods specified for ICS by NIST Special Publication 800-50 [13] consist of: interviews and questionnaires, review and assessment of current material, collection and review of general systems and major applications to identify asset owners and users (this will help identify significant ICS roles and responsibilities), review new recommendations from oversight bodies, analysis of attacks and threat events from an employee’s point of view which can indicate a need for further education and training [13].

NIST Special Publication 800-50 contains a relevant example of a needs assessment interview and questionnaire that should be modified according to the systems and applications residing in an organisational unit.

- For example, under the system hardware section regarding an employee who operates in the ICS environment, a question should be asked ‘how long at a time do you leave consultants alone with assets’.

3.1.2 Strategy Plan

Once the needs are documented, an awareness strategy plan will be developed and maintained. The plan will specify at the very least that personnel organisation-wide should be aware of the threats that pose a risk to assets and the countermeasures to oppose these threats in relation to established policies. The following questions need to be answered to produce the plan.

- The roles and responsibilities of the personnel responsible for designing, implementing, and maintaining the material are decided.
- Existing national policy guides which cover awareness training should be considered here.
- Topics to be covered for groups and individuals in the program.
  - E.g., Administrators inside the business IT network communicating via email tend to be the most vulnerable to phishing attacks and should be provided interactive material covering this issue.
- How will the awareness program be deployed?
  - This can comprise many techniques depending on the complexity of the message we are trying to get across, it includes but not limited to posters, newsletters, organisation-wide e-mail messages, Web-based sessions, in-person seminar-style delivery, outsourced computer-based simulations (e.g., Mimecast and Usecure are security awareness training providers who offer simulated phishing attacks to help users counter these attacks in real life)
- How and who will handle documentation, evidence, and feedback?
- The rate at which material and education should be given to individuals and groups.
  - For example, security awareness seminars should be recorded/delivered quarter yearly depending on recent attacks.
  - New employees and third-party consultants must undertake a fast-tracked awareness program before they are granted access to assets. This program should use current policies and standards as a guide to procuring the material.

3.1.3 Establishing Priorities

Once the strategy plan is complete and relevant personnel understand the divisions and responsibilities tasked to them, priorities must be established so a schedule can be put in place. NIST describes key factors to consider including the availability of material/resources, role and organizational impact, state of current compliance and critical project dependencies [13]. For example, a high priority item for the organisation should be the delivery of a seminar related to the unexpectable use of equipment, as this is a predominant attack vector for spreading malware employees need to ensure to management, they understand the acceptable use of USB drives among other standards

3.1.4 Setting the Bar

In summary, this section describes relating the complexity of the material to that of the position of an employee to create a standard base of knowledge. [13] specifies when setting the bar for an awareness effort there should be ‘expected rules of behaviour for using systems’ based on policies that concern the whole organisation. Once this information has been delivered clearly with acknowledgement of participation, the bar is raised, and more material is delivered related to potential threats such as the propagation of malware.
When developing and procuring education material it is integral to set the bar so individuals can receive and produce the relevant skills and competencies needed to perform their tasks without leaving the organisation vulnerable.
It is imperative that new staff undertake the security awareness program and review it within 30 days of their hire. For efficiency, recorded seminars can be beneficial in creating the bar regarding knowledge of common issues and threats that pose a risk to assets. Countermeasures to oppose these risks in relation to established policies need to be mentioned as well so personnel can grasp and implement what they have learnt [14].

3.2 Developing and procuring security awareness training

From the earlier sections there is enough information to start the development of the awareness program. To ensure this is the case, NIST [13] proposes the question “what behaviour do we want to reinforce” regarding awareness. In general, the organisation wishes to cultivate a security-first mindset that will ensure insiders are less likely to make mistakes that will leave the organisation vulnerable to attacks.

3.2.1 Awareness

As mentioned in section 3.1.3 the organisation may decide to launch an awareness campaign on a particular issue, for example, employees are noticing a high number of phishing attacks targeted toward them. To combat this threat an awareness campaign is begun immediately after receiving feedback where posters, stickers, slogans, and seminars are to be delivered regarding the threat. Similarly, educating users about the expected use of USB drives according to policy through this method is integral for preventing worms like Stuxnet to propagate and must be incorporated into the program.

A list of awareness topics to consider is listed in [13], alternatively, other low-cost solutions exist to obtain topics such as email advisories (e.g., ABB Cyber Security - Alerts & Notifications) and IT security websites providing daily updates on the latest attacks.
Vendors and other professional organisations are an effective solution for acquiring quick awareness material covering a range of material from simulated phishing attacks to detailed videos explaining threats and concepts (as of the date published, Infosec and KnowBe4 are among the most well-received) [15].

3.3 Implementing and monitoring the program

For a successful program [12] recommends that the implementation be explained to staff in detail according to the program model selected in section 3.1. These units need to provide their full support and

commitment regarding the expectations of staff to achieve expected results and acknowledge the benefits they obtain (e.g., self-actualisation and bonuses).
Techniques for delivering material have been detailed in the above sections which are based on [13] where you can obtain a full list of items.

Monitoring will be implemented in an automated fashion using 'training tracking software' such as 'Conductor Orchestrating Training' (as of date published) to maintain information regarding employees, attendance, dates, and costs. This will allow for simplified analysis and reporting of security awareness and training. Personnel that should obtain access to this system include CFOs, auditors (monitor compliance), managers, HR, CIOs, and program managers.
Once this system has been proven and implemented, tracking will be done to ensure personnel have completed their training and to further evaluate the correctness of the current awareness and training approach.
As it will be a requirement for new employees to complete a short awareness program, this system shall provide proof to management or the respective coordinator that a particular staff member has actually completed this process. Similarly, third parties such as consultants visiting the premises are to undertake a variation of this program before they are allowed access. This should establish standard regulations and security best practices such as mobile phone use in restricted areas etc.
Feedback will be completed after the development effort via questionnaires and evaluation forms provided by [12].

Summary including recommendations

Before Stuxnet, it was believed that an air-gapped and closed computer network would provide adequate protection from cyber threats. However, experts proclaim it was a highly targeted politically motivated effort which showed this countermeasure alone is not enough, as with the case in 2010 with the reveal of the Stuxnet worm. Therefore, more effort is required than ever to protect ICS networks as well as IT networks in general as worms and other malware-based attacks are getting more sophisticated there is no longer any single defence against these threats. Following a defence in depth (DID) strategy multi-layers of protection from physical perimeters to network security controls should be implemented.

- Utilizing strict policies for firewalls, IDS and IPS provide much of the security controls needed to protect and segment assets across ICS/OT and Enterprise IT networks to create an "air-gapped" architecture [3].
- Audits and regular patch management should be implemented in conjunction with the above controls to manage the risk of outdated assets and provide surveillance in detecting illegal or misused activities occurring [2].
- host-level security controls such as the whitelisting of applications should be implemented as opposed to backlisting or other "heuristic" approaches. This method provides defence against zero-day attacks which are a major vulnerability in specially designed attacks, such as the case with Stuxnet and Duqu where employees also helped propagate the malware [16,17].
- The literature shows insiders are the leading cause of breaches in data security and the best cost-effective ways to deal with this threat is through education and behavioural analytics [18]. Developing a security awareness program will not only educate staff on how to reduce risks

within their day to day operations, but it will also cultivate a security-first mindset where personnel will be conscious of the actions of possible insider threats around them thereby providing an additional layer of security [19].

References

[1] E.Knapp and J.Langill, “Hacking Industrial Control Systems,” in *Industrial Network Security*, 2nd Ed, 2015, ch.7, pp 171-207.
[2] S.Das, K.Kant and N.Zhang, “Security and Privacy in the Smart Grid,” in *Handbook on Securing Cyber-Phisical Critical Infrastructure*, M.Kaufmann, 2012, ch.25, pp.637-654.
[3] A.Teixeira, F.Kupzog, H.Sandberg and K.Johansson, “Cyber-Secure and Resilient Architectures for Industrial Control Systems,” in *Smart Grid Security*, F.Skopik and P.Smith, 2015, ch.6, pp.149-183.
[4] M.Wolf, “Cyber-Physical Systems,” in High-Performance Embedded Computing, M.Kaufmann, 2nd ed, 2014, ch.8, pp.391-413.
[5] J.Coker, “Ukrainian Energy Supplier Targeted by New Industroyer Malware.” Infosecurity-magazine.com. https://www.infosecurity-magazine.com/news/ukrainian-energy-industroyer/ (Accessed May. 11, 2022)
[6] M.Giles, “Triton is the world’s most murderous malware, and it’s spreading.” Technologyreview.com. https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/ (Accessed May. 11, 2022)
[7] Dale Peterson, ICS-Patch: A decision tree approach https://dale-peterson.com/wp-content/uploads/2020/10/ICS-Patch-0_1.pdf. 13 September 2020. [Accessed 17 May 2022].
[8] Oracle, System Administrator's Guide: Security Services https://docs.oracle.com/cd/E26505_01/html/E27224/auditov-2.html. [Accessed 19 May 2022].
[9] Stephen Mathezer, Introduction to ICS Security Part 2, https://www.sans.org/blog/introduction-to-ics-security-part-2/. 16 July 2021 [Accessed 25 May 2022].
[10] National Institute of Standards and Technology, 2015. *Guide to Application Whitelisting*. pp.3 - 14.
[11] “Manage Device Installation with Group Policy”, docs.microsoft.com. https://docs.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy (Accessed May. 24, 2022)
[12] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, "Guide to Industrial Control Systems (ICS) Security", *NIST Special Publication*, no. 800-82, 2022. [Accessed 28 May 2022].
[13] M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program", *NIST Special Publication*, no. 800-50, 2003. [Accessed 26 May 2022].
[14] S. Boon, "The Risk Of New Employees And How Security Teams Can Tackle It - Hoxhunt", *Hoxhunt.com*, 2022. [Online]. Available: https://www.hoxhunt.com/blog/the-risk-of-new-employees-for-your-security-team-and-how-to-tackle-it. [Accessed: 27- May- 2022].
[15] J. Witts, "The Top 10 Security Awareness Training Platforms | Expert Insights", *Expert Insights*, 2022. [Online]. Available: https://expertinsights.com/insights/the-top-security-awareness-training-platforms-for-businesses/. [Accessed: 26- May- 2022].
[16] J. Langill, "Mitigation Strategies for Stuxnet - SCADAhacker", *Scadahacker.com*, 2014. [Online]. Available: https://scadahacker.com/resources/stuxnet-mitigation.html. [Accessed: 27- May- 2022].
[17] G. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures", 2020. [Accessed 27 May 2022].
[18] T. Winston, "an intelligence perspective on insider threat & the unique role it plays in industrial control systems (ICS) environments", *Dragos*. [Accessed 27 May 2022].
[19] J. Matlock, "Dealing with Insider Threats: How to Repair the Weakest Link in Your Network Security", *Cyber Defense Magazine*, 2019. [Online]. Available: https://www.cyberdefensemagazine.com/dealing-with-insider-threats/. [Accessed: 27- May- 2022].