safeassign by Blackboard
(http://safeassign.blackboard.com/)

DEPT.SSC.SAFEASSIGN.... - SSC TUTORING - SAFEASSIGN FA2017

Draft SafeAssignment 07

Dinesh Nallapareddy
on Sat, Oct 14 2017, 6:28 PM

100% highest match
Submission ID: 258a57fb-619c-4fa4-ab52-f27787b0fd25

Attachments (1)

week7 paper.doc **100%**
Word Count: 2,318 Attachment ID: 182273831

week7 paper.doc

Running head:

1 CYBER SECURITY IMPROVEMENT PLAN. 2 1 CYBER SECURITY IMPROVEMENT PLAN. 11

1 CYBER SECURITY IMPROVEMENT PLAN

Dinesh Nallapareddy

Wilmington University

Introduction

3 PURE LAND WASTEWATER IS COMPANY THAT PROVIDES SERVICES REGARDING TREATMENT OF WASTE WATER WITH SPECIAL EMPHASIS BEING ON THE CHEMICAL MANUFACTURING AND BIOLOGICAL FERMENTATION. HOWEVER, RECENT REVELATIONS BY THE DEPARTMENT OF HOMELAND SECURITY AND ITS INTERNAL AUDIT SHOWS THAT THERE ARE VARIOUS

LOOPHOLES FOR INSTANCES OF CYBER SECURITY TO OCCUR. THIS PAPER WILL BE A CYBER SECURITY IMPROVEMENT PLAN FOR PURELANDWASTEWATER.

4 CURRENT STATE FOR SECURITY OF THE ICS

3 THE CURRENT STATE OF AFFAIRS IN REGARDS TO CYBER SECURITY FOR THE COMPANY IS NOT GOOD. 5 THE NETWORK DESIGN SYSTEM FOR THE PURE LAND WASTEWATER COMPANY IS A LOCAL AREA NETWORK, AND THE MAIN WEAKNESSES WITH THIS TYPE OF INTERFACE DESIGN INCLUDE; RISK OF BEING HACKED SINCE ALL THE DEVICES ARE VISIBLE ON THE NETWORK. A SINGLE ATTACK MAY RENDER THE ENTIRE SYSTEM LESS OPERATIONAL DUE TO THE NETWORKING CONSTRAINTS ASSOCIATED WITH LAN. HOWEVER, MY SUGGESTION IS THAT THE COMPANY COULD CONSIDER STRENGTHENING THE LAN BY ENSURING THAT EACH COMPUTER HAS UP TO DATE ANTIVIRUS AND DATA ENCRYPTION FEATURES ARE UPDATED ASS WHICH WOULD HELP TO CURB THE POSSIBILITY OF HACKERS ATTACKING THE SYSTEM ESPECIALLY THE KEY COMPUTER THAT CONTROLS THE SANITIZATION OF WATER BY THE CHEMICAL (FORTE & POWER, 2017).

FOR INSTANCE, SOME OF THE THREATS AND VULNERABILITIES THAT ARE FACING THE INDUSTRIAL CONTROL SYSTEMS FOR PURE LAND WASTE WATER INC. include; **5 EXPOSURE TO CYBERCRIME ACTIVITIES AND THE POSSIBILITY OF THE COMPANY PLYING DIRECT ROLE IN TERRORISM.**

3 MAJOR WEAKNESSES IN THE PHYSICAL DESIGN AND LAYOUT OF NETWORK COMPONENTS PURE LAND WASTE WATER HAS A COMPUTER NETWORK SYSTEM THAT POWERS SOME OF ITS OPERATIONS SUCH AS STORAGE OF DATA AND SUCH SIMILAR ACTIVITIES. HOWEVER, ACCORDING TO THE EVALUATION THAT IS DONE, THE COMPANY'S NETWORK SECURITY SYSTEM IS NOT THAT SECURE. THIS IS BECAUSE THE EVALUATION REPORT INDICATED THAT AT SOME POINT, THERE WERE 0% COMPLIANCE WITH THE CYBER SECURITY REGULATIONS AS PROVIDED BY THE DEPARTMENT OF HOMELAND SECURITY AND OTHER

RELEVANT SECURITY AGENCIES. THIS MEANS THAT THE COMPUTER NETWORK SYSTEM IS WEAK AND PRONE SECURITY BREACHES.

6 THREATS AND VULNERABILITIES FACING THE ICS

3 ONE OF THE THREATS FACING THE ICS IS THAT OF HACKING. THE COMPUTER NETWORK SECURITY OF THE COMPANY HAS BASIC SECURITY MECHANISMS THAT EXPOSE IT TO UNAUTHORIZED ACCESS THROUGH ACTIVITIES SUCH AS HACKING. ANOTHER THREAT IS STEALING OF CONFIDENTIAL INFORMATION BY THE EMPLOYEES WHO HAVE ACCESS TO THE DATABASE THROUGH GIVING THEIR PASSWORDS TO UNAUTHORIZED PEOPLE. ANOTHER THREAT IS THAT OF THEFT AS WAS IDENTIFIED BY THE DEPARTMENT OF HOMELAND SECURITY.

7 DESIRED FUTURE STATE

3 THE DESIRED FUTURE STATE OF THE CYBER SECURITY FOR THE COMPANY IS ONE WHERE ALL THE POSSIBLE COMMON SECURITY THREATS ARE TAKEN CARE OF. THIS IS TO ENSURE THE COMPANY COMPUTER NETWORK SYSTEM IS SECURE FROM CERTAIN COMMON SECURITY BREACHES SUCH AS UNAUTHORIZED ACCESS. THE COMPANY ALSO DESIRED TO HAVE AN INCIDENCE RESPONSE PLAN, IN CASE THE COMPANY IS FACED WITH INCIDENCE OF SECURITY BREACHES, THEY HAVE A FORMULA OF HANDLING TO THE SITUATION TO AVOID THE INCREASE DAMAGE OR IMPACT THAT SUCH INCIDENCES CAN CAUSE TO THE COMPANY.

8 PROCESSES OF PLANNING AND INDUSTRIAL INCIDENT MANAGEMENT

Response Planning

8 ONE CYBER INCIDENT RESPONSE PLANNING CONSIST OF SEVERAL BUILDING BLOCKS THAT INCLUDE RESPONSE TEAM, NEXT NEEDS AND ORGANIZATION PROCEDURES, REPORTING AND COMMUNICATIONS WITHIN THE TEAM TO VERIFY THAT THE PLAN WORKS S WELL. THERE SHOULD ALSO BE A STATE OF

REPORTING TO SUPPORT THE TEAM AND EXAMINE IF THE EVENT WILL OCCUR (ESCHELBECK, 2005).

Team organization

8 TEAMS MIGHT CONSIST OF ORGANIZED INDIVIDUALS CALLED CSIRT. THIS UNIT IS MADE UP OF INDIVIDUALS WHO ARE DEDICATED TO THE EFFORT OF CYBER WARFARE WHILE OTHERS WILL HAVE PART-TIME STAFF WITH OTHER RESPONSIBILITIES IN THE ORGANIZATION. TEAM RESPONSIBILITIES INCLUDE THE FOLLOWING;

• ACTING AS THE MAIN INCIDENT RESPONSE FOR THREATS AND RESPONSIBILITIES.

• THE TEAM WILL BE THE CLEARING HOUSE FOR ALL PREVENTION, ANALYSIS AND PROVIDING INFORMATION RELEVANT TO THE INCIDENTS.

• Developing organized policies and other procedures in the incident response

• Gathering the forensic information to support the analysis and any other legal actions

• Remediating the ICS after the incident

Setting Up Policies and Procedures While having the procedures is very necessary during the cyber attack response, some of these procedures are costly (Forte & Power, 2007). **8 MANY TYPES OF THE PROCEDURE POLICIES ARE VERY VALUABLE FOR THE IT AND CONTROL SYSTEMS. THEREFORE THE DETAILED OPERATING OPERATION PROCEDURES HAVE TO BE DEVELOPED AND IMPLEMENTED USING THE RESPONSE POLICY. THE INFORMATION SYSTEMS RELY ON THE ACCURACY, EMERGENCY, ACCURACY AND TIMELINESS OF THE POLICIES. SAMPLE POLICIES SHOULD BE AS FOLLOWS;**

• Human Resource: **8 POLICIES SHOULD BE MADE TO INCLUDE TO THE ADDRESS THE IMMEDIATE ACTIONS TO BE TAKEN ON THE EMPLOYEES AND THEIR**

ACTIONS.

• Information Disclosure: **8 THE POLICIES MUST BE DESIGNED TO ALLOW THE ORGANIZATION ADDRESS THE DISCLOSURE AND THE ACTIONS THAT SHOULD BE TAKEN IN CASE OF INFORMATION BREACH. SUCH POLICIES INCLUDE ACCEPTABLE USE, BACKUPS, PASSWORDS, GUEST ACCESS, ENCRYPTION AND DATA CLASSIFICATION.**

9 ADVANCED PERSISTENCE THREAT IMPACT AN ADVANCED PERSISTENT THREAT (APT) IS REFERRED TO AS A NETWORK ATTACK WHEREBY A HACKER GAINS ACCESSIBILITY OF A PARTICULAR NETWORK AND REMAIN THERE FOR A LONG TIME WITHOUT THE BEING IDENTIFIED BY THE SECURITY (COLE, 2012). THE ATTACK IS MAINLY CARRIED OUT FOR THE PURPOSE OF STEALING ORGANIZATION'S DATA. IN THIS CASE, THE AIM OF THE HACKER IS NOT TO DESTROY ANYTHING WITHIN THE NETWORK.

ACCORDING TO THE DEFINITION, APT IS CONSIDERED AS SYSTEM INTRUSION BY THE PEOPLE USING A COMPLEX PROCESS THROUGH THE CREATION OF E-MAILS OR MALICIOUS SOFTWARE TO ALLOW THEM TO HAVE ACCESS TO A GIVEN NETWORK BY APPLYING INDUSTRIAL CONTROL SYSTEM (MATTIOLI & MOULINOS, 2015). PROGRAMS WHICH ARE CODED IN A GOOD MANNER MAY BRING ABOUT A DISRUPTION OF A CONTROL SYSTEM WITHIN AN ORGANIZATION AND ENDS UP TRIGGERING CYBER WAR AS A RESULT OF ITS MASSIVE DESTRUCTION. STUXNET IS AN EXAMPLE OF A VERY EXCELLENT AND POWERFUL APT, AND THE DESIGNATION OF THE WORM WAS DONE BY IRAN (COLE, 2012). THIS WAS WITH THE INTENTION OF CAUSING DESTRUCTION TO SYSTEMS SUCH AS SCADA, ICS, AND PLC WHICH WERE ESPECIALLY USED BY EUROPE AND JAPAN. APT CAN ALSO BE TERMED AS A CYBER-PHYSICAL ATTACK USING SOFTWARE THAT BRINGS ABOUT DAMAGE TO PHYSICAL INFRASTRUCTURE AND HENCE THE ECONOMY IS NEGATIVELY AFFECTED (MATTIOLI & MOULINOS, 2015).

ONE SITUATION THAT TRIES TO ILLUSTRATE APT ATTACK WHICH HAS BEEN RECORDED RECENTLY, IS WHERE THE GERMAN STEEL MANUFACTURING INDUSTRY WAS INVADED. THE APT DESTROYED THE CONTROL SYSTEM OF THE PLANT INTERFERING WITH THE FIRMS' ACTIVITIES (COLE, 2012). A REPORT BY MATTIOLI & MOULINOS (2015) REVEALED THAT A COMPLEX IDEA WAS DEVELOPED BY AN INTRUDER WHICH CONTAINED A STRUCTURE SPEAR PHISHING EMAIL. BASICALLY, AN INTRODUCTION OF THE EMAIL WAS FOR THE HACKER TO EASILY OBTAIN ACCESS TO THE SYSTEM (MATTIOLI & MOULINOS, 2015). THE HIGH STANDARD POSSESSED BY THE CODE ENABLED IT TO OVERRUN THE EXISTING CODE HENCE INTERFERING WITH THE FULL FUNCTIONING OF THE SYSTEM.

When and how the event correlation process is used.

The event correlation process is used when a failure happens in the network central node. Event correlation processes are used to determine immediately the root cause of the operational problems/problems of failures that may reflect in the business of the company. It is also used to identify and parameterize the effect of failures. It also allows companies to take a practical instead of reactive attitude. It makes it easy to differentiate the most common alerts from those that may really have some considerable effect n the businesses. Lastly, it is used to allow the development of graphical rules in a drag-and-drop interface to the events and the conditions for the generation of alarms (Langill & Knapp, 2011).

Important Elements of Successful Monitoring Security Zones TCP-RST- When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set (Langill & Knapp, 2011).

Interfaces- This is a list of interfaces in the zone.

Policies- Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall.

Screens- A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another (Langill & Knapp, 2011).

Address books- IP addresses and address sets that make up an address book to identify its members so that you can apply policies to them.

10 **WHY THE INDUSTRIAL NETWORK PROTOCOLS BECOME COMMON INDUSTRIAL TARGETS INDUSTRIAL CONTROL SYSTEMS (ICS) ARE DISCOVERED EVERYWHERE FROM MECHANIZED MACHINES THAT FABRICATE PRODUCTS TO AN OFFICE BUILDING'S COOLING FRAMEWORK. BEFOREHAND, IT WAS STANDARD THAT ICS DEPENDED ON PARTICULAR OS AND PARTICULAR CORRESPONDENCE PROTOCOL. NOTWITHSTANDING, AS OF LATE, FRAMEWORK ADVANCEMENT COSTS HAVE BEEN LESSENED AND PROFITABILITY HAS BEEN ENHANCED BY ACTUALIZING SYSTEM ASSOCIATION IN LIGHT OF BROADLY USEFUL OS AND STANDARD COMMUNICATION PROTOCOL (KNAPP, 2011).**

TO CONTEND IN THE PRESENT MARKET-DRIVEN ECONOMY, ORGANIZATIONS AND ASSOCIATIONS SELECT PRODUCTIVE CONTROL FRAMEWORKS THAT CAN CONSEQUENTLY OVERSEE FORMS. ICS CAN BE FOUND IN ASSEMBLING, HANDLING OFFICES, AND EVEN POWER PLANTS, WHICH ASSUME A FUNDAMENTAL PART OF RUNNING A NATION. THEN AGAIN, THE EXPANDED EFFECTIVENESS THAT ICS PRESENT LIKEWISE INTRODUCES NEW ISSUES ON SECURITY. IN ALL ACTUALITY, DANGER PERFORMERS HAVE MUCH TO PICK UP WHEN THEY ASSAULT SUCH ORGANIZATIONS. AN EFFECTIVE ASSAULT ON ICS HAS A GENUINE EFFECT ON ANY ASSOCIATION. SOME OF THESE IMPACTS INCORPORATE OPERATIONAL SHUTDOWNS, HARMED HARDWARE, MONEY RELATED MISFORTUNE, PROTECTED INNOVATION ROBBERY, AND GENEROUS HEALTH AND DANGERS.

WEAPONIZED INDUSTRIAL NETWORK PROTOCOLS CYBER THREATS AND THEIR POTENTIAL IMPACT ON INDUSTRIAL NETWORK PROTOCOLS SECURING A MODERN SYSTEM AND THE ADVANTAGES ASSOCIATED WITH IT, ALBEIT

COMPARATIVE FROM MULTIPLE POINTS OF VIEW TO STANDARD VENTURE DATA FRAMEWORK SECURITY, DISPLAY A FEW SPECIAL DIFFICULTIES. WHILE THE FRAMEWORKS AND SYSTEMS USED AS A PART OF INDUSTRIAL CONTROL SYSTEM (ICSS) ARE PROFOUNDLY SPECIFIC, THEY ARE PROGRESSIVELY BASED UPON NORMAL FIGURING STAGES USING BUSINESS WORKING FRAMEWORKS. IN THE MEANTIME, THESE FRAMEWORKS ARE WORKED FOR DEPENDABILITY, PERFORMANCE, AND LIFESPAN. A COMMON COORDINATED ICS MIGHT BE RELIED UPON TO WORK IMMEDIATELY FOR A CONSIDERABLE LENGTH OF TIME OR EVEN YEARS, AND THE GENERAL FUTURE MIGHT BE MEASURED IN DECADES (BODUNGEN, SINGER, SHBEEB, HILT, & WILHOIT, 2017).

ASSAILANTS, DESPITE WHAT MIGHT BE EXPECTED, HAVE SIMPLE ACCESS TO NEW ENDEAVORS AND CAN UTILIZE THEM WHENEVER. IN AN AVERAGE VENTURE ARRANGE, FRAMEWORKS ARE PERSISTENTLY OVERSEEN TRYING TO REMAIN IN FRONT OF THIS QUICKLY ADVANCING DANGER, YET THESE STRATEGIES FREQUENTLY STRIFE WITH A MECHANICAL SYSTEM'S CENTER NECESSITIES OF UNWAVERING QUALITY AND ACCESSIBILITY. DOING NOTHING IS IMPOSSIBLE. ON ACCOUNT OF THE SIGNIFICANCE OF MODERN SYSTEMS AND THE CONCEIVABLY DESTROYING RESULTS OF AN ASSAULT, NEW SECURITY STRATEGIES SHOULD BE RECEIVED. MECHANICAL SYSTEMS ARE BEING FOCUSED AS CAN BE FOUND, IN ACTUALITY, CASES OF MODERN DIGITAL DAMAGE.

ALL IN ALL, THEY ARE THE OBJECTIVES OF ANOTHER DANGER PROFILE THAT USES MORE MODERN AND FOCUSED ON ASSAULTS THAN ANY TIME IN RECENT MEMORY. A SIMILARLY IRRITATING PATTERN IS THE ASCENT IN UNPLANNED OCCASIONS THAT HAVE PROMPTED HUGE RESULTS CAUSED WHEN AN APPROVED FRAMEWORK CLIENT UNWITTINGLY BRINGS DANGERS INTO THE SYSTEM AMID THEIR ORDINARY AND ROUTINE ASSOCIATE PARTICLE. THIS CONNECTION MIGHT BE TYPICAL NEIGHBORHOOD FRAMEWORK ORGANIZATION OR BY MEANS OF REMOTE FRAMEWORK OPERATION

The Future State of Security of ICS The following are proposed changes that must be made to the PureLand Water waste ICS:

1. 5 **ALL CHEMICALS AND SUBSTANCES THAT ARE LABELED CFATS SHOULD NOT BE USED IN THE INDUSTRIAL CONTROL SYSTEM OF THE COMPANY.**

2. 5 **THE COMPANY SHOULD ENSURE THAT THE NETWORK DESIGN THAT CONTROLS THE EXCHANGE OF DATA IN THE ICS IS SECURED AND THERE ARE NO POSSIBILITIES OF HAVING ADVANCED PERSISTENCE THREATS THAT CAN LEAD TO LOSS OF SENSITIVE DATA.**

3. 5 **THE INDUSTRIAL CONTROL SYSTEM SHOULD BE SUBJECTED TO CONSISTED ASSESSMENT AND AUDITING TO ENSURE THAT ALL SAFETY STANDARDS ARE UPHELD, AND THERE IS NO VIOLATION OF CFATS REGULATIONS.**

4. 5 **THE COMPANY SHOULD CONSIDER IMPLEMENTING ITS DATA BACKUP MECHANISM IN THE ICS TO MAKE SURE THAT THERE IS A COPY OF SENSITIVE DATA THAT CAN BE RELIED UPON WHEN CYBERCRIME INCIDENT STRIKES.**

5. 5 **ALL COMPANY NETWORK SYSTEMS ESPECIALLY THE ONES FOR THE ICY SHOULD CONTAIN PASSWORD AND ENCRYPTION FEATURES THAT CAN HELP TO SAFEGUARD DATA FROM BEING STOLEN.**

Conclusion

5 **IN CONCLUSION, DESPITE THE FACT THAT PURELAND WASTEWATER PROVIDES COMMENDABLE SERVICES, THE ISSUES REMAIN WHETHER THE COMPANY IS OBSERVING THE REGULATIONS PROVIDED WITH CFATS OR NOT. IT IS ESSENTIAL THAT REGARDLESS HOW WANTING THE SITUATION OF SANITIZATION OF WASTEWATER SHOULD BE, THE IMPACT OF THE OPERATION ON THE LIFE OF HUMAN BEING SHOULD BE PRIORITIZED. THIS CAN BE DONE BY ENSURING THAT NO POISONOUS CHEMICAL IS USED IN ANY ICS, AND FOR THE COMPANY, ITS SYSTEMS ARE WELL SECURED TO COUNTER CYBERCRIME**

WHICH CAN LEAD TO SABOTAGE AND CLOSURE OF THE ENTERPRISE (BEN ET AL, 2013) REFERENCES

Martin, J. (2013). 3 **BUSINESS AND TECHNOLOGY. NEW YORK CITY:** McGraw Hill.

Knapp, E. 11 **D., & LANGILL, J.** T. (2014). 10 **INDUSTRIAL NETWORK SECURITY: SECURING CRITICAL INFRASTRUCTURE NETWORKS FOR SMART GRID, SCADA, AND OTHER INDUSTRIAL CONTROL SYSTEMS.** Syngress.

5 **BEN MAHMOUD, M., LARRIEU, N., &PIROVANO, A.** (2013). 5 **RISK PROPAGATION ASSESSMENT FOR NETWORK SECURITY. HOBOKEN, N.J. ISTE LTD/JOHN WILEY AND SONS INC.**

Eschelbeck, G. (2005). 5 **THE LAWS OF VULNERABILITIES:** 8 **WHICH SECURITY VULNERABILITIES REALLY MATTER?** 5 **INFORMATION SECURITY TECHNICAL REPORT, 10(4), 213-219. HTTP://DX.DOI.ORG/10.1016/J.ISTR.2005.09.005**

Forte, D., & Power, R. (2007). 8 **PHYSICAL SECURITY, OVERLOOK IT AT YOUR OWN PERIL. COMPUTER FRAUD & SECURITY, 2007(8), 16-20. HTTP://DX.DOI.ORG/10.1016/S1361-3723(07)70105-7**

Cole, E. (2012). 9 **ADVANCED PERSISTENT THREAT: UNDERSTANDING THE DANGER AND HOW TO PROTECT YOUR ORGANIZATION.** New York: Prentice Hall.

9 **MATTIOLI, R.,& MOULINOS, K.** (2015). 9 **ANALYSIS OF ICS-SCADA CYBER SECURITY MATURITY LEVELS IN**

critical sectors. Heraklion: ENISA

Citations (11/11)

1 Another student's paper

2 Another student's paper

3 Another student's paper

4 Another student's paper

5 Another student's paper

6 Another student's paper

7 Another student's paper

8 Another student's paper

9 Another student's paper

10 Another student's paper

11 Another student's paper

Matched Text

Suspected Entry: **86% match**

Uploaded - week7 paper.doc
CYBER SECURITY IMPROVEMENT PLAN

Source - Another student's paper
CYBER SECURITY IMPROVEMENT PLAN ‘

Suspected Entry: **86% match**

Uploaded - week7 paper.doc
CYBER SECURITY IMPROVEMENT PLAN

Source - Another student's paper
CYBER SECURITY IMPROVEMENT PLAN ‘

Suspected Entry: **99% match**

Uploaded - week7 paper.doc
1 CYBER SECURITY IMPROVEMENT PLAN

Source - Another student's paper
CYBER SECURITY IMPROVEMENT PLAN 1

Suspected Entry: **91% match**

Uploaded - week7 paper.doc

Source - Another student's paper

PURE LAND WASTEWATER IS COMPANY THAT PROVIDES SERVICES REGARDING TREATMENT OF WASTE WATER WITH SPECIAL EMPHASIS BEING ON THE CHEMICAL MANUFACTURING AND BIOLOGICAL FERMENTATION	PureLand Wastewater is company that provides services regarding treatment of waste water with special emphasis being on the chemical manufacturing and biological fermentation

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
HOWEVER, RECENT REVELATIONS BY THE DEPARTMENT OF HOMELAND SECURITY AND ITS INTERNAL AUDIT SHOWS THAT THERE ARE VARIOUS LOOPHOLES FOR INSTANCES OF CYBER SECURITY TO OCCUR	However, recent revelations by the Department of Homeland Security and its internal audit shows that there are various loopholes for instances of cyber security to occur

Suspected Entry: **80% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THIS PAPER WILL BE A CYBER SECURITY IMPROVEMENT PLAN FOR PURELANDWASTEWATER	This paper will be a Cyber Security Improvement Plan for PureLand Wastewater

Suspected Entry: **86% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THE CURRENT STATE OF AFFAIRS IN REGARDS TO CYBER SECURITY FOR THE COMPANY IS NOT GOOD	Description of the Current State The current state of affairs in regards to cyber security for the company is not good

Suspected Entry: **73% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
MAJOR WEAKNESSES IN THE PHYSICAL DESIGN AND LAYOUT OF NETWORK COMPONENTS PURE LAND WASTE WATER HAS A COMPUTER NETWORK SYSTEM THAT POWERS SOME OF ITS OPERATIONS SUCH AS STORAGE OF DATA AND SUCH SIMILAR ACTIVITIES	Overview of Network Weaknesses PureLand Wastewater has a computer network system that powers some of its operations such as storage of data and such similar activities

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

HOWEVER, ACCORDING TO THE EVALUATION THAT IS DONE, THE COMPANY'S NETWORK SECURITY SYSTEM IS NOT THAT SECURE

Source - Another student's paper

However, according to the evaluation that is done, the company's network security system is not that secure

Suspected Entry: **96% match**

Uploaded - week7 paper.doc

THIS IS BECAUSE THE EVALUATION REPORT INDICATED THAT AT SOME POINT, THERE WERE 0% COMPLIANCE WITH THE CYBER SECURITY REGULATIONS AS PROVIDED BY THE DEPARTMENT OF HOMELAND SECURITY AND OTHER RELEVANT SECURITY AGENCIES

Source - Another student's paper

This is because the evaluation report indicated that tat some point, there were 0% compliance with the cyber security regulations as provided by the Department of Homeland Security and other relevant security agencies

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

THIS MEANS THAT THE COMPUTER NETWORK SYSTEM IS WEAK AND PRONE SECURITY BREACHES

Source - Another student's paper

This means that the computer network system is weak and prone security breaches

Suspected Entry: **75% match**

Uploaded - week7 paper.doc

ONE OF THE THREATS FACING THE ICS IS THAT OF HACKING

Source - Another student's paper

One of the threats is that of hacking

Suspected Entry: **92% match**

Uploaded - week7 paper.doc

THE COMPUTER NETWORK SECURITY OF THE COMPANY HAS BASIC SECURITY MECHANISMS

Source - Another student's paper

The computer network security of the company has basic security mechanisms that exposes it to unauthorized

THAT EXPOSE IT TO UNAUTHORIZED ACCESS THROUGH ACTIVITIES SUCH AS HACKING	access through activities such as hacking

Suspected Entry: **99% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
ANOTHER THREAT IS STEALING OF CONFIDENTIAL INFORMATION BY THE EMPLOYEES WHO HAVE ACCESS TO THE DATABASE THROUGH GIVING THEIR PASSWORDS TO UNAUTHORIZED PEOPLE	Another threat is stealing of confidential information by the employees who have access to the database through giving their passwords to unauthorized people

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
ANOTHER THREAT IS THAT OF THEFT AS WAS IDENTIFIED BY THE DEPARTMENT OF HOMELAND SECURITY	Another threat is that of theft as was identified by the Department of Homeland Security

Suspected Entry: **91% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THE DESIRED FUTURE STATE OF THE CYBER SECURITY FOR THE COMPANY IS ONE WHERE ALL THE POSSIBLE COMMON SECURITY THREATS ARE TAKEN CARE OF	Desired future state The desired future state of the cyber security for the company is one where all the possible common security threats are taken care of

Suspected Entry: **96% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THIS IS TO ENSURE THE COMPANY COMPUTER NETWORK SYSTEM IS SECURE FROM CERTAIN COMMON SECURITY BREACHES SUCH AS UNAUTHORIZED ACCESS	This is to ensure the company computer network system is secure for certain common security breaches such as unauthorized access

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

THE COMPANY ALSO DESIRED TO HAVE AN INCIDENCE RESPONSE PLAN, IN CASE THE COMPANY IS FACED WITH INCIDENCE OF SECURITY BREACHES, THEY HAVE A FORMULA OF HANDLING TO THE SITUATION TO AVOID THE INCREASE DAMAGE OR IMPACT THAT SUCH INCIDENCES CAN CAUSE TO THE COMPANY

Source - Another student's paper

The company also desired to have an incidence response plan, in case the company is faced with incidence of security breaches, they have a formula of handling to the situation to avoid the increase damage or impact that such incidences can cause to the company

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

BUSINESS AND TECHNOLOGY

Source - Another student's paper

Business and Technology

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

NEW YORK CITY

Source - Another student's paper

New York City

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

CURRENT STATE FOR SECURITY OF THE ICS

Source - Another student's paper

Current state for Security of the ICS

Suspected Entry: **97% match**

Uploaded - week7 paper.doc

THE NETWORK DESIGN SYSTEM FOR THE PURE LAND WASTEWATER COMPANY IS A LOCAL AREA NETWORK, AND THE MAIN WEAKNESSES WITH THIS TYPE OF INTERFACE DESIGN INCLUDE

Source - Another student's paper

Network design The system design for the Pure land wastewater company is a Local Area Network, and the main weaknesses with this type of interface design include

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

Source - Another student's paper

RISK OF BEING HACKED SINCE ALL THE DEVICES ARE VISIBLE ON THE NETWORK	risk of being hacked since all the devices are visible on the network

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
A SINGLE ATTACK MAY RENDER THE ENTIRE SYSTEM LESS OPERATIONAL DUE TO THE NETWORKING CONSTRAINTS ASSOCIATED WITH LAN	A single attack may render the entire system less operational due to the networking constraints associated with LAN

Suspected Entry: **99% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
HOWEVER, MY SUGGESTION IS THAT THE COMPANY COULD CONSIDER STRENGTHENING THE LAN BY ENSURING THAT EACH COMPUTER HAS UP TO DATE ANTIVIRUS AND DATA ENCRYPTION FEATURES ARE UPDATED ASS WHICH WOULD HELP TO CURB THE POSSIBILITY OF HACKERS ATTACKING THE SYSTEM ESPECIALLY THE KEY COMPUTER THAT CONTROLS THE SANITIZATION OF WATER BY THE CHEMICAL (FORTE & POWER, 2017)	However, my suggestion is that the company could consider strengthening the LAN by ensuring that each computer has up to date antivirus and data encryption features are updated ass which would help to curb the possibility of hackers attacking the system especially the key computer that controls the sanitization of water by the chemical (Forte & Power, 2017)

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
FOR INSTANCE, SOME OF THE THREATS AND VULNERABILITIES THAT ARE FACING THE INDUSTRIAL CONTROL SYSTEMS FOR PURE LAND WASTE WATER INC	For instance, some of the threats and vulnerabilities that are facing the industrial control systems for pure land waste water Inc

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
EXPOSURE TO CYBERCRIME ACTIVITIES AND THE POSSIBILITY OF THE COMPANY PLYING DIRECT	exposure to cybercrime activities and the possibility of the company plying direct role in terrorism

ROLE IN TERRORISM

Suspected Entry: **90% match**

Uploaded - week7 paper.doc

ALL CHEMICALS AND SUBSTANCES THAT ARE LABELED CFATS SHOULD NOT BE USED IN THE INDUSTRIAL CONTROL SYSTEM OF THE COMPANY

Source - Another student's paper

· All chemicals and substances that are labelled CFATS should not be used in the Industrial control system of the company

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

THE COMPANY SHOULD ENSURE THAT THE NETWORK DESIGN THAT CONTROLS THE EXCHANGE OF DATA IN THE ICS IS SECURED AND THERE ARE NO POSSIBILITIES OF HAVING ADVANCED PERSISTENCE THREATS THAT CAN LEAD TO LOSS OF SENSITIVE DATA

Source - Another student's paper

· The company should ensure that the network design that controls the exchange of data in the ICS is secured and there are no possibilities of having Advanced Persistence Threats that can lead to loss of sensitive data

Suspected Entry: **98% match**

Uploaded - week7 paper.doc

THE INDUSTRIAL CONTROL SYSTEM SHOULD BE SUBJECTED TO CONSISTED ASSESSMENT AND AUDITING TO ENSURE THAT ALL SAFETY STANDARDS ARE UPHELD, AND THERE IS NO VIOLATION OF CFATS REGULATIONS

Source - Another student's paper

· The industrial control system should be subjected to consisted t assessment and auditing to ensure that all safety standards are upheld, and there is no violation of CFATS regulations

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

THE COMPANY SHOULD CONSIDER IMPLEMENTING ITS DATA BACKUP MECHANISM IN THE ICS TO MAKE SURE THAT THERE IS A COPY OF SENSITIVE DATA THAT CAN BE RELIED UPON WHEN CYBERCRIME INCIDENT STRIKES

Source - Another student's paper

· The company should consider implementing its data backup mechanism in the ICS to make sure that there is a copy of sensitive data that can be relied upon when cybercrime incident strikes

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

ALL COMPANY NETWORK SYSTEMS ESPECIALLY THE ONES FOR THE ICY SHOULD CONTAIN PASSWORD AND ENCRYPTION FEATURES THAT CAN HELP TO SAFEGUARD DATA FROM BEING STOLEN

Source - Another student's paper

· All company network systems especially the ones for the ICY should contain password and encryption features that can help to safeguard data from being stolen

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

IN CONCLUSION, DESPITE THE FACT THAT PURELAND WASTEWATER PROVIDES COMMENDABLE SERVICES, THE ISSUES REMAIN WHETHER THE COMPANY IS OBSERVING THE REGULATIONS PROVIDED WITH CFATS OR NOT

Source - Another student's paper

In conclusion, despite the fact that Pureland wastewater provides commendable services, the issues remain whether the company is observing the regulations provided with CFATS or not

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

IT IS ESSENTIAL THAT REGARDLESS HOW WANTING THE SITUATION OF SANITIZATION OF WASTEWATER SHOULD BE, THE IMPACT OF THE OPERATION ON THE LIFE OF HUMAN BEING SHOULD BE PRIORITIZED

Source - Another student's paper

It is essential that regardless how wanting the situation of sanitization of wastewater should be, the impact of the operation on the life of human being should be prioritized

Suspected Entry: **98% match**

Uploaded - week7 paper.doc

THIS CAN BE DONE BY ENSURING THAT NO POISONOUS CHEMICAL IS USED IN ANY ICS, AND FOR THE COMPANY, ITS SYSTEMS ARE WELL SECURED TO COUNTER CYBERCRIME WHICH CAN LEAD TO SABOTAGE AND CLOSURE OF THE ENTERPRISE (BEN ET AL, 2013) REFERENCES

Source - Another student's paper

This can be done by ensuring that no poisonous chemical is used in any ICS, and for the company, its systems are well secured to counter cybercrime which can lead to sabotage and closure of the enterprise (Ben et al, 2013)

Suspected Entry: **92% match**

Uploaded - week7 paper.doc
BEN MAHMOUD, M., LARRIEU, N., &PIROVANO, A

Source - Another student's paper
Reference Ben Mahmoud, M., Larrieu, N., & Pirovano, A

Suspected Entry: **100% match**

Uploaded - week7 paper.doc
RISK PROPAGATION ASSESSMENT FOR NETWORK SECURITY

Source - Another student's paper
Risk propagation assessment for network security

Suspected Entry: **100% match**

Uploaded - week7 paper.doc
HOBOKEN, N.J

Source - Another student's paper
Hoboken, N.J

Suspected Entry: **100% match**

Uploaded - week7 paper.doc
ISTE LTD/JOHN WILEY AND SONS INC

Source - Another student's paper
ISTE Ltd/John Wiley and Sons Inc

Suspected Entry: **100% match**

Uploaded - week7 paper.doc
THE LAWS OF VULNERABILITIES

Source - Another student's paper
The Laws of Vulnerabilities

Suspected Entry: **99% match**

Uploaded - week7 paper.doc
INFORMATION SECURITY TECHNICAL REPORT, 10(4), 213-219

Source - Another student's paper
Information Security Technical Report, 10(4), 213-219

Suspected Entry: **86% match**

Uploaded - week7 paper.doc

HTTP://DX.DOI.ORG/10.1016/J.ISTR.2005.09.005

Source - Another student's paper

http://dx.doi.org/10.1016/j.istr.2005.09.005 Forte, D., & Power, R

Suspected Entry: **88% match**

Uploaded - week7 paper.doc

THREATS AND VULNERABILITIES FACING THE ICS

Source - Another student's paper

5 Threats and vulnerabilities facing the ICS

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

DESIRED FUTURE STATE

Source - Another student's paper

Desired Future State

Suspected Entry: **84% match**

Uploaded - week7 paper.doc

PROCESSES OF PLANNING AND INDUSTRIAL INCIDENT MANAGEMENT

Source - Another student's paper

The following shows the processes of planning and industrial incident management

Suspected Entry: **96% match**

Uploaded - week7 paper.doc

ONE CYBER INCIDENT RESPONSE PLANNING CONSIST OF SEVERAL BUILDING BLOCKS THAT INCLUDE RESPONSE TEAM, NEXT NEEDS AND ORGANIZATION PROCEDURES, REPORTING AND COMMUNICATIONS WITHIN THE TEAM TO VERIFY THAT THE PLAN WORKS S WELL

Source - Another student's paper

Response Planning One cyber incident response planning consist of several building blocks that include response team, next needs and organization procedures, reporting and communications within the team to verify that the plan works s well

Suspected Entry: **82% match**

Uploaded - week7 paper.doc

Source - Another student's paper

THERE SHOULD ALSO BE A STATE OF REPORTING TO SUPPORT THE TEAM AND EXAMINE IF THE EVENT WILL OCCUR (ESCHELBECK, 2005)	There should also be a state of reporting to support the tem and examine if the event will occur

Suspected Entry: **87% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
TEAMS MIGHT CONSIST OF ORGANIZED INDIVIDUALS CALLED CSIRT	Team organization Teams might consist of organized individuals called CSIRT

Suspected Entry: **90% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THIS UNIT IS MADE UP OF INDIVIDUALS WHO ARE DEDICATED TO THE EFFORT OF CYBER WARFARE WHILE OTHERS WILL HAVE PART-TIME STAFF WITH OTHER RESPONSIBILITIES IN THE ORGANIZATION	This unit is made up of individuals who are dedicated to the effort of cyberwarfare while others will have part-time staff with other responsibilities in the organization

Suspected Entry: **99% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
TEAM RESPONSIBILITIES INCLUDE THE FOLLOWING	Team responsibilities include the following

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
• ACTING AS THE MAIN INCIDENT RESPONSE FOR THREATS AND RESPONSIBILITIES	· Acting as the main incident response for threats and responsibilities

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
• THE TEAM WILL BE THE CLEARING HOUSE FOR ALL PREVENTION, ANALYSIS AND PROVIDING	· The team will be the clearing house for all prevention, analysis and providing information relevant to the

INFORMATION RELEVANT TO THE INCIDENTS	incidents

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
MANY TYPES OF THE PROCEDURE POLICIES ARE VERY VALUABLE FOR THE IT AND CONTROL SYSTEMS	Many types of the procedure policies are very valuable for the IT and Control systems

Suspected Entry: **97% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THEREFORE THE DETAILED OPERATING OPERATION PROCEDURES HAVE TO BE DEVELOPED AND IMPLEMENTED USING THE RESPONSE POLICY	This therefore the detailed operating operation procedures have to be developed and implemented using the response policy

Suspected Entry: **72% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
THE INFORMATION SYSTEMS RELY ON THE ACCURACY, EMERGENCY, ACCURACY AND TIMELINESS OF THE POLICIES	Therefore the Information systems rely mainly on the accuracy, emergency, accuracy and timeliness of the when the adjustments can be made

Suspected Entry: **99% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
SAMPLE POLICIES SHOULD BE AS FOLLOWS	Sample policies should be as follows

Suspected Entry: **100% match**

Uploaded - week7 paper.doc	**Source -** Another student's paper
POLICIES SHOULD BE MADE TO INCLUDE TO THE ADDRESS THE IMMEDIATE ACTIONS TO BE TAKEN ON THE EMPLOYEES AND THEIR ACTIONS	Policies should be made to include to the address the immediate actions to be taken on the employees and their actions

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

THE POLICIES MUST BE DESIGNED TO ALLOW THE ORGANIZATION ADDRESS THE DISCLOSURE AND THE ACTIONS THAT SHOULD BE TAKEN IN CASE OF INFORMATION BREACH

Source - Another student's paper

The policies must be designed to allow the organization address the disclosure and the actions that should be taken in case of information breach

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

SUCH POLICIES INCLUDE ACCEPTABLE USE, BACKUPS, PASSWORDS, GUEST ACCESS, ENCRYPTION AND DATA CLASSIFICATION

Source - Another student's paper

Such policies include acceptable use, backups, passwords, guest access, encryption and data classification

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

WHICH SECURITY VULNERABILITIES REALLY MATTER

Source - Another student's paper

Which security vulnerabilities really matter

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

PHYSICAL SECURITY, OVERLOOK IT AT YOUR OWN PERIL

Source - Another student's paper

Physical security, overlook it at your own peril

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

COMPUTER FRAUD & SECURITY, 2007(8), 16-20

Source - Another student's paper

Computer Fraud & Security, 2007(8), 16-20

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

HTTP://DX.DOI.ORG/10.1016/S1361-3723(07)70105-7

Source - Another student's paper

http://dx.doi.org/10.1016/s1361-3723(07)70105-7

Suspected Entry: **93% match**

Uploaded - week7 paper.doc

ADVANCED PERSISTENCE THREAT IMPACT AN ADVANCED PERSISTENT THREAT (APT) IS REFERRED TO AS A NETWORK ATTACK WHEREBY A HACKER GAINS ACCESSIBILITY OF A PARTICULAR NETWORK AND REMAIN THERE FOR A LONG TIME WITHOUT THE BEING IDENTIFIED BY THE SECURITY (COLE, 2012)

Source - Another student's paper

An advanced persistent threat (APT) is referred to as a network attack whereby a hacker gains accessibility of a particular network and remain there for a long time without the being identified by the security (Cole, 2012)

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

THE ATTACK IS MAINLY CARRIED OUT FOR THE PURPOSE OF STEALING ORGANIZATION'S DATA

Source - Another student's paper

The attack is mainly carried out for the purpose of stealing organization's data

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

IN THIS CASE, THE AIM OF THE HACKER IS NOT TO DESTROY ANYTHING WITHIN THE NETWORK

Source - Another student's paper

In this case, the aim of the hacker is not to destroy anything within the network

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

ACCORDING TO THE DEFINITION, APT IS CONSIDERED AS SYSTEM INTRUSION BY THE PEOPLE USING A COMPLEX PROCESS THROUGH THE CREATION OF E-MAILS OR MALICIOUS SOFTWARE TO ALLOW THEM TO HAVE ACCESS TO

Source - Another student's paper

According to the definition, APT is considered as system intrusion by the people using a complex process through the creation of e-mails or malicious software to allow them to have access to a given network by applying industrial control system (Mattioli & Moulinos, 2015)

A GIVEN NETWORK BY APPLYING INDUSTRIAL CONTROL SYSTEM (MATTIOLI & MOULINOS, 2015)

Suspected Entry: **93% match**

Uploaded - week7 paper.doc

PROGRAMS WHICH ARE CODED IN A GOOD MANNER MAY BRING ABOUT A DISRUPTION OF A CONTROL SYSTEM WITHIN AN ORGANIZATION AND ENDS UP TRIGGERING CYBER WAR AS A RESULT OF ITS MASSIVE DESTRUCTION

Source - Another student's paper

Programs which are coded in a good manner may bring about a disruption of a control system within an organization and ends up triggering cyberwar as a result of its massive destruction

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

STUXNET IS AN EXAMPLE OF A VERY EXCELLENT AND POWERFUL APT, AND THE DESIGNATION OF THE WORM WAS DONE BY IRAN (COLE, 2012)

Source - Another student's paper

Stuxnet is an example of a very excellent and powerful APT, and the designation of the worm was done by Iran (Cole, 2012)

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

THIS WAS WITH THE INTENTION OF CAUSING DESTRUCTION TO SYSTEMS SUCH AS SCADA, ICS, AND PLC WHICH WERE ESPECIALLY USED BY EUROPE AND JAPAN

Source - Another student's paper

This was with the intention of causing destruction to systems such as SCADA, ICS, and PLC which were especially used by Europe and Japan

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

APT CAN ALSO BE TERMED AS A CYBER-PHYSICAL ATTACK USING SOFTWARE THAT BRINGS ABOUT DAMAGE TO PHYSICAL INFRASTRUCTURE AND HENCE THE ECONOMY IS NEGATIVELY AFFECTED (MATTIOLI & MOULINOS, 2015)

Source - Another student's paper

APT can also be termed as a cyber-physical attack using software that brings about damage to physical infrastructure and hence the economy is negatively affected (Mattioli & Moulinos, 2015)

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

ONE SITUATION THAT TRIES TO ILLUSTRATE APT ATTACK WHICH HAS BEEN RECORDED RECENTLY, IS WHERE THE GERMAN STEEL MANUFACTURING INDUSTRY WAS INVADED

Source - Another student's paper

One situation that tries to illustrate APT attack which has been recorded recently, is where the German steel manufacturing industry was invaded

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

THE APT DESTROYED THE CONTROL SYSTEM OF THE PLANT INTERFERING WITH THE FIRMS&APOS

Source - Another student's paper

The APT destroyed the control system of the plant interfering with the firms&apos

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

ACTIVITIES (COLE, 2012)

Source - Another student's paper

activities (Cole, 2012)

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

A REPORT BY MATTIOLI & MOULINOS (2015) REVEALED THAT A COMPLEX IDEA WAS DEVELOPED BY AN INTRUDER WHICH CONTAINED A STRUCTURE SPEAR PHISHING EMAIL

Source - Another student's paper

A report by Mattioli & Moulinos (2015) revealed that a complex idea was developed by an intruder which contained a structure spear phishing email

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

BASICALLY, AN INTRODUCTION OF THE EMAIL WAS FOR THE HACKER TO EASILY OBTAIN ACCESS TO THE SYSTEM (MATTIOLI & MOULINOS, 2015)

Source - Another student's paper

Basically, an introduction of the email was for the hacker to easily obtain access to the system (Mattioli & Moulinos, 2015)

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

THE HIGH STANDARD POSSESSED BY THE CODE ENABLED IT TO OVERRUN THE EXISTING CODE HENCE INTERFERING WITH THE FULL FUNCTIONING OF THE SYSTEM

Source - Another student's paper

The high standard possessed by the code enabled it to overrun the existing code hence interfering with the full functioning of the system

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

ADVANCED PERSISTENT THREAT

Source - Another student's paper

Advanced persistent threat

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

UNDERSTANDING THE DANGER AND HOW TO PROTECT YOUR ORGANIZATION

Source - Another student's paper

understanding the danger and how to protect your organization

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

MATTIOLI, R.,& MOULINOS, K

Source - Another student's paper

Mattioli, R., & Moulinos, K

Suspected Entry: **87% match**

Uploaded - week7 paper.doc

ANALYSIS OF ICS-SCADA CYBER SECURITY MATURITY LEVELS IN

Source - Another student's paper

Analysis of ICS-SCADA cyber security maturity levels in critical sectors

Suspected Entry: **82% match**

Uploaded - week7 paper.doc

Source - Another student's paper

WHY THE INDUSTRIAL NETWORK PROTOCOLS BECOME COMMON INDUSTRIAL TARGETS INDUSTRIAL CONTROL SYSTEMS (ICS) ARE DISCOVERED EVERYWHERE FROM MECHANIZED MACHINES THAT FABRICATE PRODUCTS TO AN OFFICE BUILDING'S COOLING FRAMEWORK

Industrial Control Systems (ICS) are discovered everywhere from mechanized machines that fabricate products to an office building's cooling framework

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

BEFOREHAND, IT WAS STANDARD THAT ICS DEPENDED ON PARTICULAR OS AND PARTICULAR CORRESPONDENCE PROTOCOL

Source - Another student's paper

Beforehand, it was standard that ICS depended on particular OS and particular correspondence protocol

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

NOTWITHSTANDING, AS OF LATE, FRAMEWORK ADVANCEMENT COSTS HAVE BEEN LESSENED AND PROFITABILITY HAS BEEN ENHANCED BY ACTUALIZING SYSTEM ASSOCIATION IN LIGHT OF BROADLY USEFUL OS AND STANDARD COMMUNICATION PROTOCOL (KNAPP, 2011)

Source - Another student's paper

Notwithstanding, as of late, framework advancement costs have been lessened and profitability has been enhanced by actualizing system association in light of broadly useful OS and standard communication protocol (Knapp, 2011)

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

TO CONTEND IN THE PRESENT MARKET-DRIVEN ECONOMY, ORGANIZATIONS AND ASSOCIATIONS SELECT PRODUCTIVE CONTROL FRAMEWORKS THAT CAN CONSEQUENTLY OVERSEE FORMS

Source - Another student's paper

To contend in the present market-driven economy, organizations and associations select productive control frameworks that can consequently oversee forms

Suspected Entry: **93% match**

Uploaded - week7 paper.doc

ICS CAN BE FOUND IN ASSEMBLING, HANDLING OFFICES, AND EVEN POWER PLANTS, WHICH

Source - Another student's paper

ICS can be found in assembling, handling offices, and even power plants, which assumes a fundamental part of running a nation

ASSUME A FUNDAMENTAL PART OF RUNNING A NATION

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

THEN AGAIN, THE EXPANDED EFFECTIVENESS THAT ICS PRESENT LIKEWISE INTRODUCES NEW ISSUES ON SECURITY

Source - Another student's paper

Then again, the expanded effectiveness that ICS present likewise introduces new issues on security

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

IN ALL ACTUALITY, DANGER PERFORMERS HAVE MUCH TO PICK UP WHEN THEY ASSAULT SUCH ORGANIZATIONS

Source - Another student's paper

In all actuality, danger performers have much to pick up when they assault such organizations

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

AN EFFECTIVE ASSAULT ON ICS HAS A GENUINE EFFECT ON ANY ASSOCIATION

Source - Another student's paper

An effective assault on ICS has a genuine effect on any association

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

SOME OF THESE IMPACTS INCORPORATE OPERATIONAL SHUTDOWNS, HARMED HARDWARE, MONEY RELATED MISFORTUNE, PROTECTED INNOVATION ROBBERY, AND GENEROUS HEALTH AND DANGERS

Source - Another student's paper

Some of these impacts incorporate operational shutdowns, harmed hardware, money related misfortune, protected innovation robbery, and generous health and dangers

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

Source - Another student's paper

WEAPONIZED INDUSTRIAL NETWORK PROTOCOLS CYBER THREATS AND THEIR POTENTIAL IMPACT ON INDUSTRIAL NETWORK PROTOCOLS SECURING A MODERN SYSTEM AND THE ADVANTAGES ASSOCIATED WITH IT, ALBEIT COMPARATIVE FROM MULTIPLE POINTS OF VIEW TO STANDARD VENTURE DATA FRAMEWORK SECURITY, DISPLAY A FEW SPECIAL DIFFICULTIES

Weaponized industrial network protocols cyber threats and their potential impact on Industrial network protocols Securing a modern system and the advantages associated with it, albeit comparative from multiple points of view to standard venture data framework security, display a few special difficulties

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

WHILE THE FRAMEWORKS AND SYSTEMS USED AS A PART OF INDUSTRIAL CONTROL SYSTEM (ICSS) ARE PROFOUNDLY SPECIFIC, THEY ARE PROGRESSIVELY BASED UPON NORMAL FIGURING STAGES USING BUSINESS WORKING FRAMEWORKS

Source - Another student's paper

While the frameworks and systems used as a part of industrial control system (ICSs) are profoundly specific, they are progressively based upon normal figuring stages using business working frameworks

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

IN THE MEANTIME, THESE FRAMEWORKS ARE WORKED FOR DEPENDABILITY, PERFORMANCE, AND LIFESPAN

Source - Another student's paper

In the meantime, these frameworks are worked for dependability, performance, and lifespan

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

A COMMON COORDINATED ICS MIGHT BE RELIED UPON TO WORK IMMEDIATELY FOR A CONSIDERABLE LENGTH OF TIME OR EVEN YEARS, AND THE GENERAL FUTURE MIGHT BE MEASURED IN DECADES (BODUNGEN, SINGER, SHBEEB, HILT, & WILHOIT, 2017)

Source - Another student's paper

A common coordinated ICS might be relied upon to work immediately for a considerable length of time or even years, and the general future might be measured in decades (Bodungen, Singer, Shbeeb, Hilt, & Wilhoit, 2017)

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

ASSAILANTS, DESPITE WHAT MIGHT BE EXPECTED, HAVE SIMPLE ACCESS TO NEW ENDEAVORS AND CAN UTILIZE THEM WHENEVER

Source - Another student's paper

Assailants, despite what might be expected, have simple access to new endeavors and can utilize them whenever

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

IN AN AVERAGE VENTURE ARRANGE, FRAMEWORKS ARE PERSISTENTLY OVERSEEN TRYING TO REMAIN IN FRONT OF THIS QUICKLY ADVANCING DANGER, YET THESE STRATEGIES FREQUENTLY STRIFE WITH A MECHANICAL SYSTEM'S CENTER NECESSITIES OF UNWAVERING QUALITY AND ACCESSIBILITY

Source - Another student's paper

In an average venture arrange, frameworks are persistently overseen trying to remain in front of this quickly advancing danger, yet these strategies frequently strife with a mechanical system's center necessities of unwavering quality and accessibility

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

DOING NOTHING IS IMPOSSIBLE

Source - Another student's paper

Doing nothing is impossible

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

ON ACCOUNT OF THE SIGNIFICANCE OF MODERN SYSTEMS AND THE CONCEIVABLY DESTROYING RESULTS OF AN ASSAULT, NEW SECURITY STRATEGIES SHOULD BE RECEIVED

Source - Another student's paper

On account of the significance of modern systems and the conceivably destroying results of an assault, new security strategies should be received

Suspected Entry: **99% match**

Uploaded - week7 paper.doc

MECHANICAL SYSTEMS ARE BEING FOCUSED AS CAN BE FOUND, IN ACTUALITY, CASES OF MODERN DIGITAL DAMAGE

Source - Another student's paper

Mechanical systems are being focused as can be found, in actuality, cases of modern digital damage

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

ALL IN ALL, THEY ARE THE OBJECTIVES OF ANOTHER DANGER PROFILE THAT USES MORE MODERN AND FOCUSED ON ASSAULTS THAN ANY TIME IN RECENT MEMORY

Source - Another student's paper

All in all, they are the objectives of another danger profile that uses more modern and focused on assaults than any time in recent memory

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

A SIMILARLY IRRITATING PATTERN IS THE ASCENT IN UNPLANNED OCCASIONS THAT HAVE PROMPTED HUGE RESULTS CAUSED WHEN AN APPROVED FRAMEWORK CLIENT UNWITTINGLY BRINGS DANGERS INTO THE SYSTEM AMID THEIR ORDINARY AND ROUTINE ASSOCIATE PARTICLE

Source - Another student's paper

A similarly irritating pattern is the ascent in unplanned occasions that have prompted huge results caused when an approved framework client unwittingly brings dangers into the system amid their ordinary and routine associate particle

Suspected Entry: **96% match**

Uploaded - week7 paper.doc

THIS CONNECTION MIGHT BE TYPICAL NEIGHBORHOOD FRAMEWORK ORGANIZATION OR BY MEANS OF REMOTE FRAMEWORK OPERATION

Source - Another student's paper

This connection might be typical neighborhood framework organization or by means of remote framework operation References

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

INDUSTRIAL NETWORK SECURITY

Source - Another student's paper

Industrial network security

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

SECURING CRITICAL INFRASTRUCTURE NETWORKS FOR SMART GRID, SCADA, AND OTHER INDUSTRIAL CONTROL SYSTEMS

Source - Another student's paper

Securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems

Suspected Entry: **100% match**

Uploaded - week7 paper.doc

D., & LANGILL, J

Source - Another student's paper

D., & Langill, J