Safety practice

Understanding and managing cyber security threats and countermeasures in the process industries

Dr Andrea Longley, Chemical Industries Association, UK

Summary

A number of case studies relating to cyber attacks resulting in physical damage to process plant are presented. The good cyber hygiene practices which could have thwarted the attacks are outlined. General introductions to the concept of cyber security management systems, control system architecture, identification of vulnerabilities, countermeasures and mitigations are provided, and key cyber security learnings are detailed.

Keywords: Cyber security

Introduction

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, software and data from attack, damage or unauthorised access. It incorporates protection of internet-connected systems, including hardware, software and data, from cyber attacks. For the process industries, this means process control and safety systems together with their connections to business enterprise systems, which are the systems often connected to the internet itself. Good cyber hygiene is encouraged so that opportunities for attack are reduced. A lifecycle and robust management system approach to cyber security is recommended and physical security is considered part of such a system.

Cyber attacks have been shown to impact process plant hardware operations through manipulation of operating conditions resulting in physical damage.

Businesses have many drivers to increase the connectivity between process control systems (or operational technology – 'OT') and business enterprise systems (or information technology – 'IT'). Often these drivers facilitate improvements in production and maintenance efficiencies. In process safety for example, there are great benefits brought when process safety key performance indicators (PSMKPI) can automatically access and directly report key process data. Such direct reporting enables powerful information to reach the necessary people in organisations in real time with reduced risk of error. This data can then be acted on in a timely fashion to help reduce the risk of process safety incidents. Such beneficial connectivity, however, brings with it greater potential attack space opportunity.

Cyber attacks impacting the OT environment have the potential to result in both loss of business continuity and hazardous loss of control leading to loss of containment, equipment damage or loss of an essential utility supply. Loss of business continuity or loss of intellectual property can result from attacks in the IT environment, aimed towards for example, extortion or reconnaissance for future OT attack. Copies of P&IDs or operating procedures could be valuable to an attacker planning a future OT attack. The average time to detect intrusion into a corporate network is measured in months.

Background

The awareness of the importance of cyber security for chemical and manufacturing sites is rapidly increasing but greater appreciation at senior management levels of the business risk it represents still needs to be appreciated. Cyber attacks are regularly reported in the news and with the recent implementation by HSE of cyber security intervention plans for COMAH[1] sites as well as sites subject to the Network Information System Regulations for Operators of Essential Services[2], there is the growing realisation that sites should be prepared to defend themselves against attacks which could result in unwanted malicious manipulation of physical process plant. Such attacks would include deliberate or inadvertent destruction, or loss of confidence in the safe operation of the control system or process plant. Where sites use computerised process control networks to control processes with major accident hazard potential, the consequence of a successful and unmitigated cyber attack could be intolerable.

An example of a cyber attack causing physical sabotage

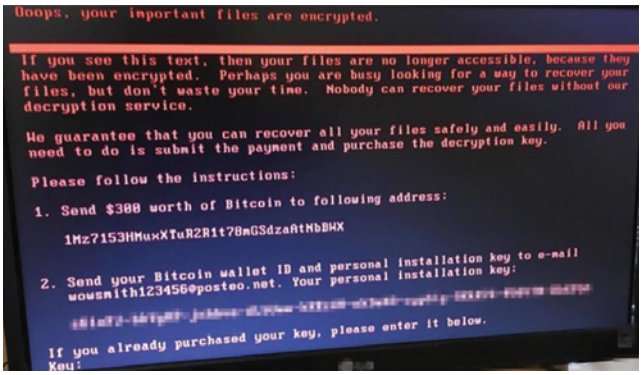


Figure 1 – Ransom demand following cyber-attack

0260-9576/19/$17.63 + 0.00

is Stuxnet[3]. This is the name of a computer virus, malicious software (malware) or 'cyberworm' that is thought to have infected control systems in the Natanz uranium enrichment facility in Iran in 2010. It is believed to have altered the Siemens SCADA control software, which enabled operating conditions of computer-controlled centrifuges to be changed, causing them to be destroyed and thus require replacement. It did this by simultaneously altering the speed of the centrifuges and providing false data feedback to operators on the control displays so that the deviations would not be detected. The virus is understood to have been introduced to the computer systems via an infected USB stick. Iran subsequently admitted its nuclear programme operations had been delayed. This is a real example of operational damage or delay caused by malicious cyber intervention of process plant. If replicated in a chemical business, it could cause a range of unacceptable consequences from business disruption to major incidents.

It is a misconception that to counteract cyber attacks requires only specialised technological expertise. Cyber security is a management issue too and site management should ensure that a cyber security management system is in place. It is about recognising deliberate and/or malicious intent, targeted or widespread, either from external or internal attackers, either by ignorance, chance or design. Cyber security seeks to:

- Identify systems potentially at risk;
- Protect those systems from unauthorised manipulation;
- Detect unauthorised access or modifications to those systems;
- Respond to attacks or threats to minimise loss;
- Recover from any successful attack.

Case study examples

A cyber attack affecting the public occurred in Ukraine in December 2016[4] when a power cut caused the loss of about 20% of Kiev's power consumption for just over an hour. This followed a previous similar event in 2015 that cut off thousands of consumers and simultaneously bombarded customer service phones with fake calls so that genuine customers could not report the cut. It is understood that the company was set up such that staff could log onto the electricity management system (OT environment) from the enterprise IT environment via just a username and password. This attack relied on malware known as BlackEnergy3 which is believed to have been delivered via email using a technique known as 'spear phishing'[5]. Spear phishing is said to have occurred when information taken from social media is used to make 'phishing' emails more convincing and therefore less likely to arouse suspicion. In this case, the malware gave attackers remote access to computer systems, allowing them to flip circuit breakers to cut the power.

A further example of a cyber attack generating physical damage is provided by the German steel mill case study[6]. In this instance, a spear phishing email is reported to have enabled access to corporate networks and then moved into the plant network. Multiple plant process components including a furnace were subsequently physically damaged and caused to fail. It is likely that internal reconnaissance techniques such as keyloggers or network scanning would have been used to enable the crossover from corporate network to plant network. It is recommended that any connections between corporate and plant networks should be controlled through the use of what is termed a 'demilitarized zone' (DMZ) with firewalls, monitoring and defence systems as well as tight physical access control. Network security monitoring would have allowed quick detection of any attackers' movements or scanning activities within the plant network. Further, physically engineered standalone safety systems such as independent high temperature trips can provide a further layer of protection which will be unaffected by cyber attacks and thus ultimately reduce the risk of event escalation.

A ransomware attack was reported in 2017[7] when a cyber attack knocked out the Windows based systems that monitor nuclear radiation around the Chernobyl nuclear plant. This attack originated in Ukraine and spread to several other firms including the Maersk Group and Cadbury. US$300 of Bitcoin payments were demanded to recover encrypted files. This attack exploited a flaw in the Windows software for which Microsoft had released a patch to fix but the suggestion is that this patch was not deployed by the affected companies.

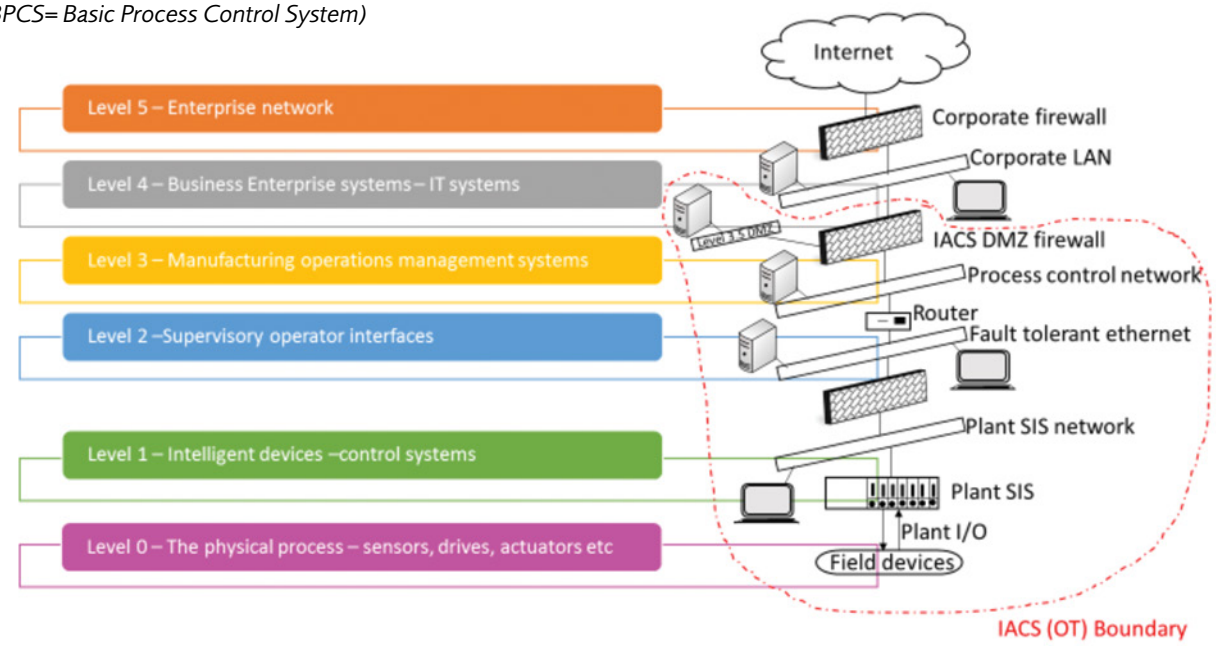
In May 2017 the National Health Service in the UK was also hit[8] by the WannaCry ransomware which resulted in an estimated 19,000 appointments, including operations, being cancelled. It was reported that NHS trusts had not patched or upgraded vulnerable software and that the attack was extremely unsophisticated and could have therefore been easily avoided by keeping up to date with upgrades and timely implementation of software patches.

In December 2017 it was reported[9] that an attacker deployed malware designed to manipulate an industrial safety system at a critical infrastructure organisation. This attack, named TRITON, is built to interact with Triconex Safety Instrumented System (SIS) controllers. It is designed to prevent safety mechanisms from executing their intended function, resulting in actual physical damage and potentially harm. The incident occurred by remote access to an engineering workstation which was then reprogrammed. Some SIS controllers moved to a failed safe state which automatically shutdown the process. The investigation found that the SIS controllers initiated a safe shutdown when application code between processing units failed a validation check. The safe shutdown was unlikely to have been the intention of the attack. The concern is that the attacker targeted the SIS, suggesting an interest in causing a high-impact attack with physical consequences. For several years now, increasing integration between control systems and SIS has occurred for reasons including cost reduction, time savings, and benefits of data exchange. The TRITON attack acutely demonstrates the resulting risk from allowing such two-way communications and the National Cyber Security Centre (NCSC) subsequently issued a paper[10] on how to detect and recommended steps to mitigate against disruption from such an attack.

These case study examples demonstrate the real threat to existing process plants and the importance of good cyber security management. Countermeasures need not necessarily rely on advanced technology and good cyber hygiene, supported by an effective cyber management regime, can be an effective first line of defence.

0260-9576/19/$17.63 + 0.00

Figure 2 – Simplified Purdue diagram showing control system architecture (BPCS= Basic Process Control System)



System architecture

While basic steps such as physical security around access to industrial control systems and effective management systems are important, other aspects such as system architecture, access control, data security and network and system resilience should also be considered.

HSE's Operational Guidance Document OG86 Edition 2[11] sets out the Safety Regulator's planned inspection initiative to check that sites subject to the Control of Major Accident Hazard (COMAH) Regulations have measures in place to prevent major accidents from occurring due to malicious manipulation of Industrial Automation & Control Systems – IACS – common in industrial process plant. The guidance provides significant information on providing cyber security for industrial automation and control systems (IACS) and further information on cyber security is available on the HSE's website[12]. Essentially, the recommendation is to implement a Cyber Security Management System (CSMS) and build appropriate cyber security competences. The scope of the control system should be identified, and its architecture grouped into zones, connections between zones documented and a risk assessment process used to determine proportionate expectations for countermeasures which consider major accident hazard risk. Due to the nature of attacks with malicious intent, a normal risk assessment process incorporating a frequency based likelihood is not appropriate and sites are encouraged to judge risk and then adopt appropriate cyber standards dependant on a combination of potential consequence, system vulnerability, attractiveness of target, criticality of the system preventing the consequence and such like.

It is good practice for companies to be able to clearly define boundaries between OT and IT to demonstrate understanding of their own network architecture. Purdue diagrams are helpful to show connections right through a computer network to help identify vulnerabilities and determine appropriate countermeasure protection.

The diagram above includes a DMZ or demilitarised zone at level 3.5, which is a sub-network that contains and exposes external-facing services to a larger and less trusted network. The DMZ can store process information which can subsequently be accessible from the corporate IT systems as necessary for such applications as PSMKPI reporting or process and maintenance monitoring. If properly configured, the DMZ protects against an external attacker gaining access to the control system. Appropriate network architecture, segregation and access countermeasures are all required at each level. These defences act as layers of protection, making attacks more difficult and slowing down an attacker, thus increasing the likelihood of detection followed by containment and eradication prior to any unwanted consequences occurring.

With an understanding of which control systems are being used to protect against major accident hazards, combined with an understanding of potential threats and vulnerable connection routes, appropriate countermeasure protection and mitigations can be prioritised for implementation through an improvement programme where necessary.

Lessons

Achieving the necessary levels of resilience is not easy and takes both time and commitment. It is however essential to providing business resilience. While there will be much 'devil in the detail' to cover, sites should consider a lifecycle approach to cyber security, developing their own policy and procedures on cyber standards and expected countermeasures or mitigations, undertaking a gap analysis and developing a plan of how to address the gaps, all as part of an overarching CSMS. The basic framework based on lessons from operational experience can be built around the following steps:

Identify

It is essential to prepare an asset register and simplified

0260-9576/19/$17.63 + 0.00

network drawing such as a Purdue level diagram to describe the system scope and architecture and facilitate identification of vulnerabilities.

Normal risk assessment techniques incorporating likelihood-based modifiers are not appropriate for cyber security issues and protection, detection and response measures should be provided using a standards-based approach related to consequence and criticality, rather than being based on conventional overall risk, which cannot be predicted.

Organisational responsibilities which include governance and cyber security competence management should be considered as part of the CSMS within the overall Safety Management System.

Protect

Sites should be aware that some existing safety related layers of protection may not work under abnormal cyber attack situations, for example, an operator's response may not be what is needed if their control system display has been hacked to show false information. Independent protection layers should be considered for major accident hazard prevention.

Eventually, required cyber integrity levels should be developed for cyber attack scenarios which link to major accident scenarios and enable prioritisation of upgrade actions in any improvement programme that is developed. In the interim, proportionate countermeasures should be defined and implemented that consider cyber threat scenarios.

Sites should implement good cyber hygiene measures (the 14 principles of which are listed in the HSE's Operational Guidance[11] Appendix 2 pp20-32): patching systems, controlling internet connectivity, controlling remote access and scanning or restricting USB sticks and ports etc..

Cyber security requirements should be included on project specifications. This would encourage vendors to resolve any vulnerabilities. Sites are recommended to improve their awareness and understanding of this topic so that they can be intelligent customers. HR teams should include cyber threat considerations when undertaking personnel screening and recruitment.

Under no circumstances should systems with a physical key access to 'program' modes be left in this mode during plant operation and adequate management of change measures should be in place to alert appropriate personnel in the event of any oversights in relation to this.

An inherent safety approach is to use mechanical controls such as locked control system cabinets and interlocks and reduce attack space by reducing terminals and removing ports for USB sticks although it is recognised this may not result in the most efficient system. Equally it is important to give people the right tools for them to do their jobs, otherwise they will invent work-arounds which may be counterproductive.

Detect

Adoption of system monitoring techniques to detect attack activities as well as hunting for threats are recommended to provide dual assurance of cyber security.

Respond

Cyber security management systems (CSMS) should be implemented which detail incident management and recovery. Plans should be in place on how to operate without systems. Timely containment and eradication will minimise impacts.

Recover

Sites should have a recovery plan with backups available for control systems to enable timely restoration of lost or corrupted data and software.

Conclusions

Security will be improved by separating operational technology (OT) environments from information technology (IT) environments – i.e. separation of the industrial automation or plant control networks from general business networks by physical separation or firewalls and a DMZ (demilitarised zone). Segregation of OT and IT is however just one part of designing an overall defensive architecture. Other activities to deliver robust organisational countermeasures (scope definitions, roles and responsibilities, management of change, cyber competency, access control etc) are also important to facilitate understanding of vulnerabilities and failure mechanisms which then enables appropriate countermeasures to be implemented.

It is important to remember that controlling physical access can be as important with cyber security as connectivity access ('logical access'). Access should be controlled to a minimum for both physical and digital systems. Unnecessary connections, applications and services should be removed (collectively known as 'system hardening'), a robust risk-based vulnerability management process should be in place and good backups should be regularly made with restore procedures easily followed. While difficult to achieve in the OT environment, all the latest security updates and patches should be applied in a timely manner at least for the IT environment. A good cyber security management system with appropriate management of change procedures are essential to reducing cyber attack opportunities.

Cyber security is a rapidly changing topic. There is a need to predict developments and react quickly. Leadership from site senior management teams should be visible as awareness and vigilance by all staff is a key requirement. Sites should be encouraged to build competency and create a culture of security awareness.

References

1. *HSE. The Control of Major Accident Hazard Regulations 2015. [Online] 2015. http://www.hse.gov.uk/pubns/priced/l111.pdf.*
2. *The Network and Information Systems Regulations 2018. [Online] 2018. https://www.legislation.gov.uk/uksi/2018/506/made.*
3. *Arthur, Charles. The Guardian. [Online] 26 Feb 2013. https://www.theguardian.com/technology/2013/feb/26/symantec-us-computer-virus-iran-nuclear.*
4. *BBC News. BBC News. Ukraine power cut 'was cyber attack'. [Online] 11 January 2017. https://www.bbc.co.uk/news/technology-38573074.*
5. *Spear Phishing. National Cyber Security Centre blog post.*

0260-9576/19/$17.63 + 0.00

[Online] 16 May 2018. https://www.ncsc.gov.uk/blog-post/phishing-spear-phishing-and-whaling-does-it-change-price-phish.

6. *R. M. Lee, M. J. Assante, T. Conway. ICS-CPPE - case study 2 German Steelworks Facility. ICS SANS. [Online] 30 December 2014. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.*
7. *Duckett, Adam. Hack hits Chernobyl monitoring system. The Chemical Engineer. [Online] 28 June 2017. https://www.thechemicalengineer.com/news/hack-hits-chernobyl-monitoring-system/.*
8. *BBC News. BBC News. NHS 'could have prevented' WannaCry ransomware attack. [Online] 27 October 2017. https://www.bbc.co.uk/news/technology-41753022.*
9. *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. FireEye. [Online] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.*
10. *Centre, National Cyber Security. TRITON Malware Targeting Safety Controllers. NCSC. [Online] https://www.ncsc.gov.uk/information/triton-malware-targeting-safety-controllers.*
11. *HSE. Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2. HSE Internal Ops. [Online] http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf.*
12. *Cyber Security. HSE . [Online] http://www.hse.gov.uk/eci/cyber security.htm.*

Further information

BSI. BS EN 61511-3:2017 Functional safety. Safety instrumented systems for the process industry sector. BSi Standards Publication. [Online]

BSi. BS EN 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. BSi Standards Publication. [Online]

ISO. ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management. ISO. [Online]

ISA. ISA/IEC 62443 Cybersecurity Certificate Programs. [Online]

GIAC. Global Industrial Cyber Security Professional (GICSP). GIAC Certifications. [Online] https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp.

NCSC. NIS Guidance Collection. NCSC NIS Guidance. [Online] https://www.ncsc.gov.uk/collection/nis-directive.

Leverett, Éireann. Cyber Insurance for Civil Nuclear Facilities. chathamhouse.org. [Online] 8 May 2019. https://reader.chathamhouse.org/cyber-insurance-civil-nuclear-facilities-risks-and-opportunities#.

The Association of German Engineers. VDI-Standard: VDI/VDE 2182. VDI. [Online] https://www.vdi.eu/nc/guidelines/vdivde_2182_blatt_1-informationssicherheit_in_der_industriellen_automatisierung_allgemeines_vorgehensmode/.

0260-9576/19/$17.63 + 0.00