CYBER SECURITY INSIGHTS FOR INDUSTRIAL & AUTOMATED CONTROL SYSTEMS (IACS)

CHEMICAL-PROCESSING INDUSTRIES REPORT

Volume 1 | Issued May 2018 | Author: Ian Gemski, Tekgem

TABLE OF CONTENTS

FOREWORD

As the industry body representing North East England's chemical-processing sector, NEPIC play a vital role in supporting manufacturers in the face of its challenges. By developing a collaborative business environment that promotes sustainability and growth, we have brought a wide range of inter-related industries together to tackle change, overcome barriers and source solutions.

The 4th Industrial Revolution represents an extraordinary growth opportunity for manufacturing in general, however, by its very nature brings with it increased jeopardy. A recent report highlighted that almost 50 per cent of manufacturers have been victim to cyber security, with a quarter suffering some financial loss or disruption.

Manufacturing is now the 3rd most targeted sector for attack behind Government systems and finance. Much of this vulnerability arises from industrial systems installed on plants that have built up and been modified over several years and, in some cases, decades. Whilst there is no change to the data collected, collated and used, the data management systems differ, resulting in an integration challenge to produce real time, meaningful information whilst protecting the asset.

NEPIC welcomes the Health & Safety Executive's (HSE) response to the severity of this challenge through the introduction of operational guidelines for industrial automated control systems. However, more needs to be done to raise awareness and understanding of the challenges involved in devising and implementing a cyber security strategy that will enable chemical companies to take the appropriate steps to protect themselves.

By bringing chemical manufacturers together with the HSE, and the technology firms leading the way in cyber security in the region, we have collectively enabled not only the findings and recommendations of this initial report but have taken the first steps toward creating an effective cyber security culture throughout the cluster.

I take this opportunity to thank event partners Tekgem and the Health and Safety Executive for their expert knowledge and guidance as we come together to understand the changing environments and be clear on which risks pose the biggest danger to our organisations whilst maximising the extraordinary potential that technological advances offer.

Philip Aldridge

Philip Aldridge
Chief Executive, NEPIC

EXECUTIVE SUMMARY

March 2017 was a tipping-point for the UK's chemical-processing industries as the Health and Safety Executive (HSE) – in response to the increasing number of cyber-attacks against critical national infrastructure (CNI) – introduced new Operational Guidelines for Industrial Automated Control Systems (IACS).

In response, Tekgem who've spent the last decade working with organisations of all sizes from across the chemical-processing industries in the field of IACS cyber security and the North East Process Industries Cluster (NEPIC) came together to build an IACS community. The key objective of the initiative was to create a knowledge hub where the HSE, chemical-processing companies, duty-holders, operators, services providers, suppliers and technology vendors could come together and share their knowledge and experience.

On the 22nd March 2018 NEPIC hosted an IACS Cyber Security event at the Wilton Centre on Teesside that saw Sarabjit Purewal and Nic Butcher (Health and Safety Executive), Ian Gemski (Tekgem), Tony Porritt (SABIC) and Michael Stubbings (Frazer Nash) address an audience that ranged from Instrument & Control Engineers to IT/OT Support Technicians, Automation & DCS Managers to Engineering Directors – all of whom are currently working on chemical-processing plants.

The event highlighted the need for all parts of the chemical-processing industry to come together in order to effectively manage the ever-evolving threat of cyber-attack, whether malicious or accidental.

The purpose of this report isn't to summarise each and every cyber security threat. Instead, it discusses the key threats and risks facing the chemical-processing sector that were pinpointed during the event. In addition, the report offers recommendations on how to defend against and respond to the IACS cyber security threats highlighted by panel members during the event's Q & A session.

SECTION 1

IACS OPERATIONAL GUIDELINES

While the UK's chemical processing industries haven't yet fallen victim to a publicised cyber-attack, the HSE introduced the IACS Operational Guidelines because a regulatory and technical framework to guard against such attacks did not exist.

The reality of the situation is this. There are currently a large number of chemical-processing plants who are relying on legacy IACS infrastructures, plants which were never conceived with cyber security or IP connectivity in mind.

However, such automation has delivered huge improvements in terms performance, and no one can afford for it to be lost or compromised, either by cyber-attack or poorly thought-out cyber security measures.

Taking that into account, one of the key objectives set out by the HSE was to ensure that the IACS Operational Guidelines would offer a baseline from which organisations can implement cyber security processes, standards and training to successfully manage the health and safety risks resulting from a cyber-attack.

Beyond this initial objective, both Sarabjit and Nic stated during the event that the IACS Operational Guidelines will evolve over time and it's their intention to work closely with the National Cyber Security Centre (NCSC) and all relevant parties across the chemical-processing sector to ensure the next iterations of the IACS Operational Guidelines are fit-for-purpose.

In fact, it was clear from the event that both Sarabjit and Nic understand there is a great deal of variety in the level and sophistication of automation in chemical manufacturing processes, as well as a great many different attitudes and cultures in terms of cyber security.

With that in mind, they and the HSE are well aware that the chemical-processing sector is not presently built for a generalist response to cyber security challenges, and this point was reinforced with an announcement from Sarabjit during his talk that the next version of the IACS Operational Guidelines will be realised later this year.

SECTION 2

MALICIOUS CYBER-ATTACKS

Notable IACS cyber security trends

Looking beyond the headline-grabbing cyber security incidents of recent years, this section of the report includes threat intelligence gathered from the NCSC and global chemical companies, along with the insights and examples outlined in Nic Butcher's (HSE) presentation at the recent IACS event. This analysis has exposed the following key IACS cyber-security threats:

'Watering Hole' cyber-attack

In this example of a cyber-attack, Nic described how the malicious attacker used a 'watering hole' attack to compromise a supplier to a COMAH operator.

The attacker crafted a 'spear-phishing' email which was sent from the supplier's system. The email contained Malware which gave the attacker command and control of the COMAH operator's enterprise desktop. The attacker then spread laterally across the COMAH operator's corporate network, securing persistent access.

The next step of the attack was to acquire the technical information – network design documents, ICS documents, P&ID, maintenance schedules, passwords for key systems – needed to attack the system.

Once the attacker had the credentials he began the process of acquiring the knowledge of the network to penetrate deeper into the control system.

In this instance, the attacker intercepted and modified MODBUS over TCP/IP communications between the tank farm PLC and DCS. The attacker then overrode the SIS which resulted in material being covertly pumped to overfill the jetty tank.

SECTION 2

Triton cyber-attack

In 2017 a malicious cyber-attack was carried-out on a petrochemical plant in Saudi Arabia that resulted in the attackers gaining control over a safety system that was critical in defending against catastrophic events.

Following the attack, Schneider Electric SE, the company that produces the safety instrumented system, analysed the code used in the attack and uncovered the malicious software, dubbed Triton. Triton allowed the hackers to manipulate Schneider devices' memory and run unauthorised programs on the system by leveraging the previously unknown bug.

This recent attack also highlighted a worrying change of focus by hackers. The previous Stuxnet cyber-attacks had focused on industrial control systems, but the Triton code targeted safety-instrumented systems. These safety systems can act as one of the last lines of defence when a chemical plant is facing dangerous situations that could lead to explosions or spills.

At this point, it's important to mention that the Triton code attacked older Schneider devices and wouldn't work on newer versions. However, industry experts have claimed that there are still thousands of older devices being used.

WannaCry ransomware cyber-attack

In May 2017 WannaCry hit the headlines when attackers held the NHS to ransom for its patient data, causing outrage and chaos in equal measure.

The WannaCry cyber-attack had potentially serious implications for the NHS and its ability to provide care to patients. It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice.

However, Ciaran Martin, head of the UK's NCSC, warned earlier this year that similar WannaCry ransomware cyber-attacks on the UK is a matter of "when, not if", raising the prospect of devastating disruption to critical national infrastructure.

One reason for Martin's bleak outlook could be the be down to the fact that the WannaCry attack on the NHS drew attention to the danger of using outdated operating systems, as the ransomware was designed to attack vulnerabilities in historic versions of Windows.

In fact, the use of outdated systems is common in industrial control systems, with many chemical and petrochemical facilities still relying on Windows XP or earlier versions, which have publicly known vulnerabilities and are no longer supported by Microsoft or security applications.

All of which would leave any such company lacking the technology and skilled Information Security personnel to secure systems, detect incidents, or mitigate or remediate breaches.

State sponsored cyber-attacks

In recent years allegations of state-sponsored cyber-attacks have occurred within the Middles East region with probably the Saudi Aramco attack being the most well-known.

The Saudi Aramco cyber-attack was carried-out in 2012 using a virus known as Shamoon. The Shamoon virus disrupted computers by overwriting the Master Boot Record, making it impossible for them to start up.

Former U.S. Defense Secretary Leon Panetta described the 2012 Shamoon attack on Saudi Aramco as probably the most destructive cyber-attack on a private business. The malware attack took down 35,000 systems and destroyed the records of nearly 40,000 computers and during the attack images of a burning U.S. flag were used to overwrite the drives of victims including Saudi Aramco and RasGas Co Ltd.

More recently, in late 2016, Shamoon reappeared attacking six different Saudi organisations – including the Sadara Chemical Company, a joint venture between Saudi and US companies – and overwriting target computers with the famous image of the body of Alan Kurdi, a Syrian refugee who drowned in the Mediterranean.

SECTION 3

ACCIDENTAL CYBER SECURITY INCIDENT

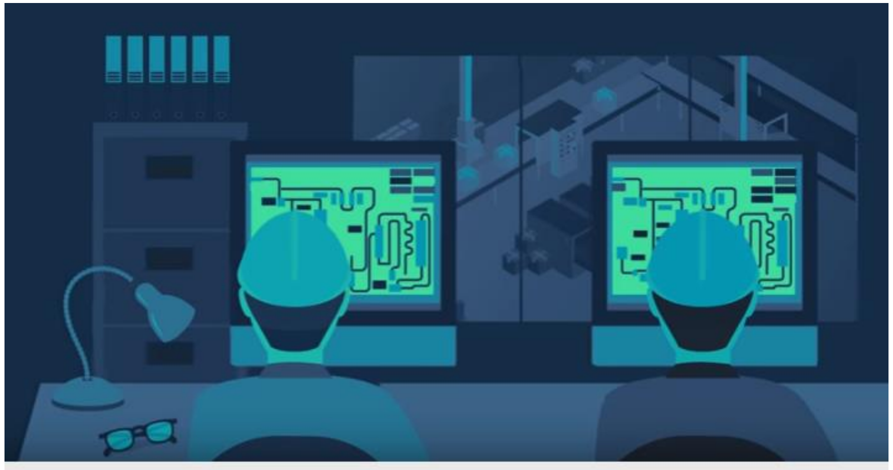
While ransomware cyber-attacks continued to make the headlines in recent years, accidental breaches caused by employee error or network-breaches prompted by third party suppliers continue to be a major threat to the effectiveness of IACS cyber security within the chemical-processing industries.

An example of such an incident was described during the event and highlighted the just how close a chemical-processing company – with sites across the globe – came to a catastrophic failure that would have impacted 80 servers and 200 database systems.

The accidental incident occurred as two plants were in the middle of a turnaround following an incident that had been raised with a vendor regarding unsupported hardware.

While the vendor supplied replacement hardware they also provided incorrect procedures for the installation of the new hardware. This in-turn caused a major hardware failure and data corruption and although a major disaster recovery was implemented, this was further hindered with issues with backups.

However, the complete loss of plant functionality was avoided in the main through effective communication between the Applications & Infrastructure team and the business, plant managers, control rooms & thirds party service providers. Once all parties had understood and agreed on the immediate business needs, they were able to prioritise the restoration for key systems in order of importance.



SECTION 4

RECOMMENDATIONS

IACS cyber security is critical if the UK's chemical-processing plants are to maintain the high-levels of productivity and safety currently being achieved. However, the insights shared at the IACS event alongside industry-specific IACS threat intelligence is proof that being aware of a cyber security threat is not enough to prevent a catastrophic cyber-attack.

Ultimately, if the chemical-processing industry is to sustain its success, users, suppliers, service providers and vendors must first understand and identify each and every cyber security vulnerability within an organisation. Once the risk is understood all parties can begin to undertake the relevant steps needed the meet the HSE's new IACS Operational Guidelines for cyber security.

In order to achieve that objective experience has shown that effective and efficient IACS cyber security strategies are achieved by implementing a 'Defense-in-Depth' approach. However, for this strategy to realise the results required, businesses must ensure that *'people and process'* sit at the core of their approach.

Worryingly, in many cases the first step organisations take to protect themselves against cyberattacks is to buy a raft of new security products. However, knee-jerk acquisitions of technology don't deliver, either in terms of ROI or securing your business.

What organisations should do is increase the levels of cyber security training for all personnel – internal and external – that have access to the network. In addition, businesses must invest time and money to improve their internal cyber security and operational processes.

With that in mind, the following top-line recommendations outline where an organisation could begin its journey towards effective and efficient IACS cyber security were identified and highlighted.

SECTION 4

RECOMMENDATIONS - PEOPLE

The introduction of the new IACS Operational Guidelines and the ever-increasing threat of cyber-attack has created a significant increase in interest on the topic of cyber security, with stories of organisations spending large sums of money to protect themselves against a fast-evolving array of current and potential future threats.

For many the response is to spend heavily on monitoring, surveillance and software. However, they often neglect the risk exposure created by their own people – and, in this digital age, by their employees, customers, suppliers, service providers and technology vendors.

The Watering Hole cyber-attack we highlighted began with a spear-phishing email which targeted a supplier. To guard against such attacks businesses from top to bottom, not simply the in-house IT team, must have a better understanding of the people who are accessing their networks and systems within their plants.

The reality is we're living in a hyper-connected world. IoT devices can have the potential for hidden and sometimes serious cyber security vulnerabilities. In fact, IoT devices is a fast-growing cyber security issue as more and more lifestyle mobile (smartphone) & IoT (smartwatch) devices come onto the market and are then innocently brought inside organisations.

However, no matter how secure a company's IT security platform is, the company is only as secure as its user base. Unfortunately, compromised credentials represent the vast majority of social engineering and spear phishing attacks that result in the majority of network breaches.

So, with all the investment capital devoted to securing IT infrastructure, how can companies prevent employees from opening phishing emails? The best answer is continuous, hands-on cyber-security awareness training for all relevant people who have access to the network and critical operating infrastructure.

For example, train your people to spot what good emails look like. Try to teach and show them what bad emails tend to look like. To coincide with that teaching program, it's advised to carry-out regular testing.

Perform phishing testing across your organisation to gauge end users level of sophistication at handling phishing attempts. This will help you know if users recognise these and how they're dealing with them. Also test the people in charge of managing your systems and networks to see if they are adequately enforcing the policies.

Cyber security awareness training is what will reduce the success of attacks and testing will make sure security and/or management know how to respond to them.

Beyond training users and operators, it's paramount to build diverse teams. This should include access to IACS cyber security specialists. By adopting this approach you'll have the relevant skills and experience that is tailored to the needs of your business, process control and technologies.

It's clear that the threat is evolving at a rapid rate and it's essential to have an agile team along with the necessary external support and resources whenever needed. Utilising expertise from third parties is an efficient and effective option to acquiring the right skills and experience in-house. Ultimately good people working to the right processes and standards will make the difference.

SECTION 4

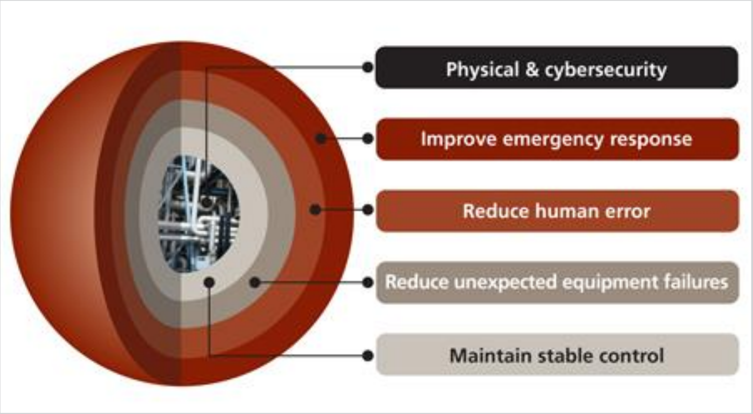
RECOMMENDATIONS - PROCESS

To have IACS cyber security-ready 'people' is a crucial element of any successful 'Defence-in Depth' approach. Nevertheless, only by establishing and maintaining the correct cyber security processes will you ensure that your organisation meets the HSE's required IACS Operational Guidelines.

While cyber security awareness training is essential, it's supremely important to assess how, what and where people are accessing the systems and networks as well as sensitive information.

In the case of the Watering Hole attack the supplier's access to systems and documents should have been monitored, with processes and restrictions put in pace to alert duty holders to any unauthorised access. Another preventative step would be to encrypt key documents and information and implement access control.

Having said that, as was the case with the Watering Hole, Triton and Shamoon attacks, it's very likely that a determined attacker would be able to breach those security measures. At this point, the increased use of programmable systems and the convergence of technologies used for industrial automation control systems (IACS) and IT systems has left a growing number of cyber security vulnerabilities that stretch far beyond the people working in and around the plants.



Unfortunately, this issue is coupled with the fact that attackers have increased capability and access to hacking hardware and software 'toolkits' and coordination that is growing by the day. All of which has left the HSE to estimate that in many chemical-processing plants the average time to detect intrusion into your corporate network is months.

Although this paints a very bleak picture, there are some organisations that have taken the lead in developing new 'Defence-in-Depth' cyber security processes to combat current and future threats.

To achieve this, some organisations have moved to a proactive, rather than reactive ‘defence-in-depth’ approach. This in part has been driven by the growing number of high profile vulnerabilities and exploits that are being discovered on a regular basis. While a vulnerability is much different to an exploit, if there is an exploit then there is a more credible threat.

However, that is not to say because there are no known exploits then you can ignore it. Because no one wants to be the first to be attacked by an unknown exploit. But a disclosed vulnerability without a credible exploit can buy you more time to patch and in turn combat the threat.

Unfortunately, patches can have the potential to cause the same impact as a virus or malware attack if not properly managed. In fact, it’s been the case that recently released patches have caused system instability and in some case crashes, unbootable devices and decreases in plant performance.

So, the question is, do you wait for the next patch to be released in the hope that the known issues are fixed, and no more known issues appear? All the while you are vulnerable to exploits that the patches are protecting against.

If you don’t patch for reasons above then you are stuck in limbo. To mitigate this you can have a sample group of systems where you can test patches as this can reduce risk and gain confidence and a better understanding of the issues you’re facing. The testing should consist of ensuring reliability and performance is not affected.

Also, use vendors where-ever possible for direction and certified testing (let them do the hard work), but don’t completely rely on them alone. Finally, have a policy and processes in place with patching framework that you can follow to aid in making decisions whether to patch or not.

Unfortunately, regardless of the fact that all of your correct patching processes are in place and implemented, sometimes disasters do and will happen. And please don’t think it will never happen to you.

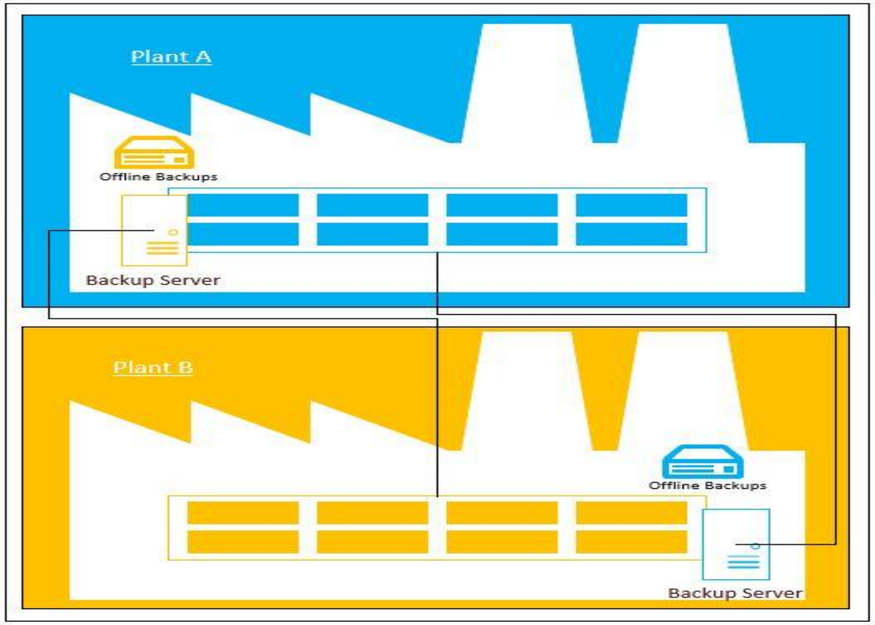
In such an instance, backups are a last line of defence when disaster strikes. When designing backup, restore and disaster recovery architectures, plan for single point of failures. It’s mission critical that you put your backup data in a different physical geographical location to production systems.

Also, you must ensure the backup servers are protected against the same vulnerability as production systems. This can be achieved with new backup software protection technologies that protect against ransomware encrypting the backup data.

Furthermore, we’d recommend using offline backups and keep another copy of your backup data off the network (SAN or NAS or even cloud) that is physically disconnected after the extra backup copy is completed.

Without any doubt it’s paramount to have a process in place - and one that is tested - which demonstrates that your backups are reliable, successful and restores when required. The last thing you want to do is go to restore and be unable to do so.

The final piece in a proactive 'defence-in-depth' approach involves establishing processes for the people who'll be involved in disaster recovery. Now, this may seem like overkill but just take a moment and try and visualise the steps you'd need to take in the event of disaster.



Do you have defined roles and responsibilities for internal and external teams? And, if as is generally the case, an attack or incident happens in the early hours of the morning, would you be able to set up lines of communication with the business, plant managers, control rooms in order to understanding the immediate needs of the business. And at a local and international level.

If you have all of the above in place well done. But, would you know which person would be ultimately responsible for the decision to prioritise the restoration for key systems in order of importance?

While that all sounds very dramatic, there's help at hand. The advent of new cloud technologies has played a key role in allowing businesses to be more proactive and test their disaster recovery capabilities.

With that in mind, the most important piece of advice in terms of disaster recovery is don't wait. The biggest mistake most companies make is waiting until after a cyberattack or disaster to figure out what to do next.

SECTION 5

CONCLUSION

The past two years has shown the chemical-processing community how significantly the cyber-attack threat is evolving as well as the need for operational guidance from HSE.

Cyber criminals can now leverage less sophisticated methods to infect machines and in some cases, extort ransoms from victims, with ransomware being used in a wide range of cybercrime activity, including email phishing campaigns and destructive attacks like WannaCry.

Beyond the threat from malicious cyber-attacks, the chemical-processing industry has to adapt to the threat of accidental cyber-security breaches that in many cases are being encountered on a much more regular basis than malicious attacks.

Chemical-processing organisations that adopt security hygiene methods, implement best practices underpinned by cyber resilience and incident response plans, employ the right mix of people and processes for dealing with the various threat scenarios and attacks described, could at least, minimise damage and impact from them.

However, the next two years is a crucial time for the chemical-processing industry as the HSE begins to roll-out its full audit program across the UK.

Put simply, it's no longer a case of meeting your internal standards for cyber security. The audits will be rigorous and comprehensive as the HSE will be using IEC/ISA standards as benchmarks within their cyber security audits and organisations will have to demonstrate compliance.

Fortunately, it's not all bad news. The chemical-processing industry already has some of the most safety conscious people working within in it. And once these people are given the support needed, they'll be able to adapt and incorporate the required IACS cyber security standards within their existing strategies without any negative impacts on the plant's performance or its safety.

SECTION 6

CREDITS & REFERENCES

AUTHOR

Ian Gemski
Managing Director
Tekgem

SOURCES

Sarabjit Purewal
Principal Specialist Inspector Cyber Security
Health & Safety Executive

Tony Porritt
Applications & Infrastructure Manager
SABIC UK Petrochemicals

Nic Butcher
HM Specialist Inspector EC&I
Health & Safety Executive

Michael Stubbings
Principal Consultant
Frazer Nash

NEPIC & Tekgem make no warranties, express or implied, with respect to the information presented here.