Cyber Security and Process Safety

An ISC Executive Briefing Paper

Paper Number 2. March 2020

"There are only two types of companies: those who have been hacked and those that will be hacked."[i]

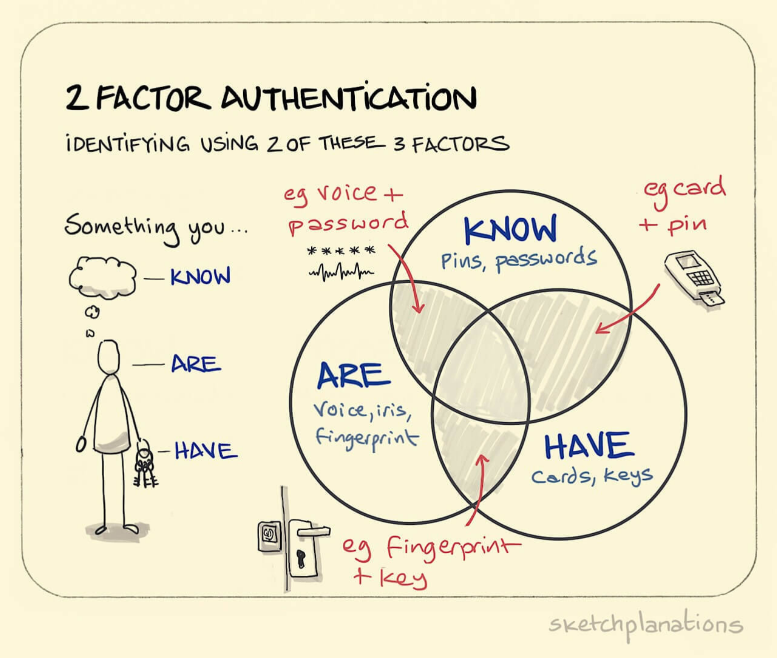
At this time this seems like a startling quote, but it is likely that very soon following this a more accurate quote would have been "There are only two types of companies: those who have been hacked and those that don't know they have been hacked." Such is the cyber landscape we live in.

Introduction

When we think about cyber security, we often think of personal data security. Additionally, from a processing plant perspective, we often comfort ourselves in the knowledge that the control system is isolated from the internet, and therefore assumed to be "safe". However, neither of these assumptions are accurate when we consider the process safety implications. There are a range of different ways an organisation's process safety can be compromised from a cyber-attack.

This paper will highlight a number of recent cyber-attacks and what should be considered from a process safety perspective. It will not provide advice on cyber security strategies, such as two factor authentication or firewalls etc; this needs to be sought from a competent cyber security professional. There are excellent resources to assist with this, such as the ISA/IEC 62443 series of standards, which provide a framework to manage security.

Specific acronyms are defined at the end of this document.



[ii]

Case Studies

There have been a number of high-profile cases in the past that have had direct process safety implications over the past 20 years. Some of these have been attacks on hardware, safety instrumented systems, control systems or enterprise information. These are detailed in Table 1.

Year	Incident	Impact
2000	Maroochy Shire Sewage Plant[iii]	A disgruntled former contractor gained access to the control system at several pumping stations in the network. This was done remotely via the radio control system. At one stage the network released 264,000 gallons of raw sewage into the community.
2010	Stuxnet Iran Nuclear Facility[iv]	Spread via a USB stick, the Stuxnet virus infected Programmable Logic Controllers (PLC) and sent damage inducing instructions to plant equipment, at the same time sending false feedback to the main controller. Making it difficult to see the plant equipment was misbehaving. It caused several centrifuges in Iran's nuclear enrichment facility to spin out of control to destruction.
2012	Saudi Aramco spear phishing[v]	Malware was installed when an employee clicked on a link in an email. It started to wipe the hard drives of 35,000 Saudi Aramco computers. This impacted their ability to do business as all enterprise systems were isolated or infected. At the time they claimed it did not impact their production, but the lack of enterprise information may have had some safety implications. Note there is no suggestion this risk occurred, this just highlights possible process safety implications.
2012	Flame virus[vi]	Similar to Stuxnet, spread via USB sticks. It recorded Skype conversations, logged keystrokes and collected screen data. Resulting in the capture of potentially safety related information.
2015	Ukraine power network[vii]	Spear-phishing was used to install malware to obtain access to the control systems after first accessing the corporate network. The attack allowed the hacker to access the control system and lock out the operators while they shut down multiple sub stations on the power network, cutting electricity to more than 230,000 people for up to 6 hours in winter.
2016	Ukraine power network[viii]	One year after the 2016 Ukraine power network attack, the network was again attacked and shut down some of the electricity supply to Ukraine for one hour.
2017	Triconex Safety System attack[ix]	Triconex is a safety instrumented system, often operating as a final line of defence for a safety incident. The Triton Malware allowed the hacker to gain remote access to the Triconex workstation. It was discovered when some controllers entered a fail-safe

		mode and shutdown. It was likely the hackers were exploring how the system worked when they tripped out some equipment.
2018	Shamoon[x]	This virus hit Saipam, the Italian oil and gas services company. It was a variant of the malware that struct Saudi Aramco in 2012 (above) but it overwrote files with random information. It only impacted the business network, and not control systems, but this may have been a safety impact from the perspective of safety critical data being overwritten. Note there is no suggestion this risk occurred, this just highlights possible process safety implications.
2019	Hydro Ransomware[xi]	Access was gained via an employee opening an infected email some months prior to the incident. This access allowed the hackers to spread a ransomware virus throughout the network. The attack lead to all computer systems being disconnected or infected. Some facilities continued operations in a manual mode, whole other sites had to shut down as the virus spread to the control systems of the plant. This attack spread across 170 facilities in 40 countries. Communication with employees was via Facebook and WhatsApp.
2020	Toll MAILTO	Toll logistics company was infected with the MAILTO ransomware, which terminates multiple processes and services buy appending random extensions to files. Toll shut down their whole network, relying on manual dispatch data. A risk here could have been not knowing the location real time of dangerous goods cargoes, making them vulnerable to hijack or not having the ability to dispatch dangerous good cargos with the correct safety information. Note there is no suggestion either of these risks occurred, this just highlights possible process safety implications.

Note this is not an exhaustive list, merely illustrative of the types of attacks that have occurred.

From the examples listed above we can see there is some clear safety implications with some of the incidents. In Maroochy, Stuxnet, both Ukraine and the Triconex examples, the hacker was able to remotely operate the facility and control the equipment. In the Saudi Aramco and Shamoon example, files were wiped from the systems or corrupted. In the Flame example, files and data were collected by the hackers. In the Hydro and Toll example, all files and data were locked and held ransom. Access to perpetrate these attacks included use of infected USB sticks, access via hacking radio control frequencies and clicking or opening an infected email, attachment or link. New virus variants emerge frequently, with a new example, EKANS being identified in early 2020. This impacts industrial control systems through ransomware targeting specific applications, such as data historians and removing process visibility from control systems.

Process Safety Implications

To understand the process safety implications, it is first important to define what the process safety critical equipment and data is. This is known as identifying the 'crown jewels'. There are many systems and collections of data that have process safety implications. Examples could be; safety instrumented systems such as emergency shut down systems, control systems where a hacker could gain access and subvert plant operations, systems data such as information contained in the knowledge management system, including operating procedures, risk assessments, management of change records, equipment drawings, maintenance scheduling, maintenance history and equipment data sheets.

In process safety risk assessments, we would determine what are the safety critical elements and work to ensure they have integrity, however when considering cyber security this list may grow to things beyond just the critical elements. For example, the maintenance scheduling system would not typically be considered a safety critical element but consider if it was infiltrated and the scheduling frequencies were altered, leaving safety critical elements to continue operating outside their risk-based test frequency. Or simply wiping the testing information or history or holding the system to ransom preventing the maintenance from taking place. How do you continue to operate safely without knowing the test status of your safety critical equipment? While this may sound farfetched for such a specific act to occur, consider the examples in the table above where there were targeted attacks. In most instances the hackers had access in the background for some time before doing something that led to their discovery.

What can you do?

Know your data and how it is protected

An Australian telecommunications provider, Telstra, has developed the 'Five Knows of Cyber Security'[xii]. This can help you think through what your 'crown jewels' are from a process safety perspective and how it is protected. There are also sever other publications that may be helpful and have been listed in the More information section of this paper.

The five knows are defined as follows;

1. Know the value of your data,
2. Know who has access to your data,
3. Know where your data is,
4. Know who is protecting your data, and
5. Know how well your data is protected.

Applying these to process safety requires some knowledge of how your process safety systems interact and work. Generic systems are described below:

Know…	Hardware and control systems	Data systems
The value of your data	Control systems such as DCS, PLC or SCADA Safety Instrumented Systems Equipment with inbuild data loggers	Enterprise knowledge management systems such as: Maintenance Management System (scheduling, tracking,

		defining maintenance activities) Operating procedures Risk assessments Plant drawings Equipment datasheets
Who has access to your data	Operators, maintainers, engineers, other employees, contractors, suppliers. Designated 'Admin' or 'Super Users'	Operators, maintainers, engineers, other employees, contractors, suppliers. Designated 'Admin' or 'Super Users'
Where your data is	Is the plant data kept locally on a network, on a stand-alone system or in the cloud? How is access to the equipment controlled?	Is the system data kept locally on a network, on a stand-alone system or in the cloud? How is access to the servers containing data controlled? Is there a manual back up system in the vent of data loss?
Who is protecting your data	Who is physically guarding your facility? Who is controlling access to the equipment data?	Who is guarding your servers or the cloud? Who is controlling access to the system data?
How well your data is protected	How easy is it to access and change equipment set points?	How easy is it to access and change systems data?

Understand the risk

Other things to consider include what is being called Risk Velocity[xiii]. This is a third dimension to standard risk assessment. Traditionally we have talked about the likelihood and the consequence when determining the risk. However, it is important to consider the speed with which the hazard moves to the consequence, because this is your mitigation window. In typical process safety the risk velocity can vary from very slow to very fast. For example, internal corrosion may take many years to develop into a pin hole, or a line could be struck by a vehicle and immediately rupture. With cyber security it can also be slow or fast. A hacker may gain undetected access to the domain and remain there undetected collecting information or learning how a process works and then may strike without warning, or it could be an immediate DDOS attack, taking your domain offline. Depending on the threat the velocity needs to be considered so that mitigation and recovery plans can be developed and tested.

Monitor and test your defence systems

Part of the system preparation and development of response and recovery plans monitoring the cyber security systems. This includes tracking the attempted and successful attacks as well as the integrity of the defence systems. To adequately do this extensive penetration testing should be conducted periodically. It is also important to consider changing your penetration testers periodically to ensure that you are getting the best possible results from the exercise.

Understand where you may have unintended consequences

In the face of a cyber threat it can be tempting to lock systems down so tight that no one can access them. However, this may in fact create additional vulnerabilities because if it is too difficult to follow the correct process, people will find work arounds. An example might be if it is too difficult for an equipment supplier to monitor their own equipment performance on your facility, they may install a workaround using a Wi-Fi router direct from their equipment. This could be a vulnerability as their equipment is connected to other plant equipment and in effect provide a back door. So, in an attempt to keep systems secure, if it is too hard to follow the process, work arounds may create an unintended consequence.

Conclusion

The world of cyber security is a complex one that requires specialist people working to develop prevention, identification and response strategies, but there is still a role for senior leaders to monitor the performance and ensure that process safety implications, which may not be immediately apparent are taken into account.

More information

There are many sources of good information regarding cyber security. Contact your local association for company directors for information or reading material on training courses for a senior executive level. For detailed cyber security advice, consider contacting a consultancy that specialises in cyber security advice, planning and penetration testing. Some other publications that may be useful are listed below:

Cyber Security for Industrial Automation and Control Systems (IACS), Edition 2.
https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

Fighting the Fight. https://www.thechemicalengineer.com/features/fighting-the-fight/

Dr. Andrea Longley. *Understanding and managing cyber security threats and countermeasures in the process industries,* Loss Prevention Bulletin Issue 268, page 2-6.

ISA/IEC62443 Series of standards.

This information is provided in good faith, but without any liability on the part of IChemE or the IChemE Safety Centre.

Acronyms

DCS – Distributed Control System

DDOS – Distributed Denial of Service

PLC – Programmable Logic Controller

SCADA – Supervisory Control and Data Acquisition

[i] *2012 attributed to Robert S Mueller III former Director of the FBI*

[ii] Source: https://www.sketchplanations.com/post/175913353056/2-factor-authentication-two-factor accessed 4th February 2020

[iii] Sayfayn, N. Madnick, S. Cybersafety Analysis of the Maroochy Shire Sewage Spill, Sloan School of Management, MIT, 2017

[iv] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html accessed 30 January 2020

[v] https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676 accessed 29 January 2020

[vi] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html accessed 30 January 2020

[vii] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ accessed 29 January 2020

[viii] https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report accessed 29 January 2020

[ix] https://www.reuters.com/article/us-cyber-infrastructure-attack/hackers-halt-plant-operations-in-watershed-cyber-attack-idUSKBN1E8271 accessed 29 January 2020

[x] https://www.zdnet.com/article/shamoon-malware-destroys-data-at-italian-oil-and-gas-company/ accessed 7 February 2020

[xi] https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ accessed 30 January 2020

[xii] https://www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf accessed 30 January 2020

[xiii] https://www.pwc.com/sg/en/risk-assurance/assets/ra-sid-risk-velocity.pdf accessed 30 January 2020