Regulatory compliance and cyber threats:

Industrial security in the pharmaceutical sector

www.copadata.com
sales@copadata.com

zenon
do it your way

Contents

In 2010, the first digital weapon aimed at industrial automation equipment changed the realm of security forever. Rather than targeting IT infrastructure like most viruses at the time, the malicious computer worm Stuxnet compromised programmable logic controllers (PLCs), collected information on industrial systems and damaged the centrifuges of the Natanz uranium enrichment plant in Iran. Stuxnet was the alarm bell that made industry aware of cyber security vulnerabilities.

Today, more industries are seeing an increasing number of cyber security threats. To tackle these issues, companies have to change the way they operate and put cyber security at the very heart of the business. We are already seeing this shift in the rise of the Chief Information Security Officer and in an increasing awareness of best industry practice when it comes to cyber security.

According to the Global State of Information Security Survey 2016, respondents increased their information security budgets by 24 per cent within the past year, which reflects a greater willingness to invest in keeping facilities secure.

The pharmaceutical industry is no different. As an attractive target for cyber attacks, pharmaceutical companies need to understand cyber security, assess weak points and implement the appropriate security measures. This white paper describes some of the most effective industrial security tools pharmaceutical companies have at their disposal in the era of Industry 4.0.

1. Pharmaceutical production: limited to limitless

Control systems for pharmaceutical production used to be proprietary and limited to the individual research and production facility. This meant a typical industrial control system would not be directly connected to the internet and therefore couldn't be easily accessed externally. However, an increasing need for automation and robotics, remote access and factory-wide connectivity has meant pharmaceutical production and control systems have changed significantly in the last decade.

The wide scale introduction of the Industrial Internet of Things (IIoT) is the next major step towards a fully connected smart factory. The benefits of the IIoT-enabled pharmaceutical production facility are clear for anyone to see. Collecting and strategically interpreting

production data using analytics and turning this information into insight can create a basis for enhancing productivity and reducing errors, in line with industry regulations and key business goals.

So how can pharmaceutical companies leverage the benefits of these new technologies while minimising the security risks?

2. The risk

Bitsight, an organisation that measures how vulnerable companies and industries are to cyber attacks, reported that cyber security attacks on the healthcare and pharmaceutical industries have worsened at a faster rate than other industry sectors. With the average 'clean up' time for these sectors following a cyber attack at just over five days, there is certainly some cause for concern.

Similarly, a report by OCISIA, in collaboration with the UK information intelligence experts, BAE Systems Detica, estimated the cost of cybercrime to the UK economy to be around £27 billion annually. The same report named the pharmaceutical and biotech sectors amongst the hardest hit industries.

In the eyes of a cyber criminal, the pharmaceutical industry provides a treasure trove of valuable information. Organisations within the sector – from drug distribution companies to research and development units – can hold highly sensitive material, from personal patient data to confidential research on drug development and testing. This makes the pharmaceutical industry an attractive target for cyber attacks.

However, it is important to remember that there are security risks involved in any manufacturing facility, particularly a smart one. An increased amount of sensors collecting production data might help monitor and understand the process better, but this type of connectivity also provides more opportunities for hackers to infiltrate the system. However, to better protect themselves from cyber attacks, pharmaceutical companies can use regulatory compliance as the first defence against cyber security.

3. Protection through compliance

When operating in one of the most heavily regulated industries in the world, pharmaceutical companies need to abide by complex laws, regulations and guidelines. Sometimes, these can become the basis for an effective industrial security strategy.

Laws within the pharmaceutical industry are often deliberately vague. Published in general terms to meet the current and future needs of the industry, pharmaceutical laws are vastly different to the guidelines that accompany them. Passing a new law is a lengthy process; regulatory guidelines on the other hand, can be implemented and adopted relatively quickly.

The Food and Drug Administration (FDA) 21 CFR Part 11 is one of the most established regulations within the industry. The regulation requires organisations to implement controls, electronic audit trails and systems validations. It establishes the standard expectations for industrial security through reliable electronic documentation of the pharmaceutical manufacturing process.

Since its introduction, there have been concerns that FDA 21 CFR Part 11 could discourage innovation and technological advances in the industry. However, compliance with this regulation is not just about ticking boxes. For the most part, the requirements of FDA 21 CFR Part 11 go hand in hand with the security necessities of modern manufacturing facilities.

By reviewing historical documentation and records, organisations can detect where security breaches have occurred and in turn, identify and protect the more vulnerable points in the system better. This way, engineering and manufacturing data is protected against unauthorized access, modification or deletion to ensure accuracy, consistency, and completeness. Ultimately, successful FDA 21 CFR Part 11 compliance will result in a more organised, efficient and secure production process.

In basic terms, Electronic Records provide secure data. Authenticated electronic signatures ensure both operators and supervisors can identify themselves in a safe and secure way when making any changes in the production process.

Combined with the implementation of smart machines and the resulting influx of big data, achieving regulatory compliance in the industry is not an easy task. To fulfil the requirements of these complex regulations and protect their facilities, smart pharmaceutical manufacturers are turning to validation-friendly applications and industrial software.

4. Smart SCADA security

Intelligent SCADA software, like COPA-DATA's zenon, ensures a HMI/SCADA system is compliant with industry regulations, and provides built-in cyber security capabilities. This "Security by Design" approach means the software and its components are specifically designed to guarantee secure operations.

Built in software security features that protect companies against data loss and unauthorised access include a file signature functionality that recognises manipulated program files, strong encryption, secure authentication and automatic synchronisation of files in the network with "click-and-forget technology".

Integrated user administration, for example, ensures unauthorised users cannot gain control of equipment. It means most user operations can be locked, even access to Windows Desktop. This way, if a security breach *does* occur, it can be easily contained and access to other applications can be prevented.

Best practice also dictates that pharmaceutical manufacturers should encrypt valuable data. This could mean compressing production data and sending it through the network and to web clients in an encrypted form, as well as ensuring passwords are encrypted to protect project data and expertise.

Some HMI/SCADA software uses its own network protocol to communicate between the individual software products. This way, data can be transferred to separate binary data packages and machine-readable information in plain text is never communicated in the complete communication concept. Further client authentication at the connection set up stage also prevents access to the network.

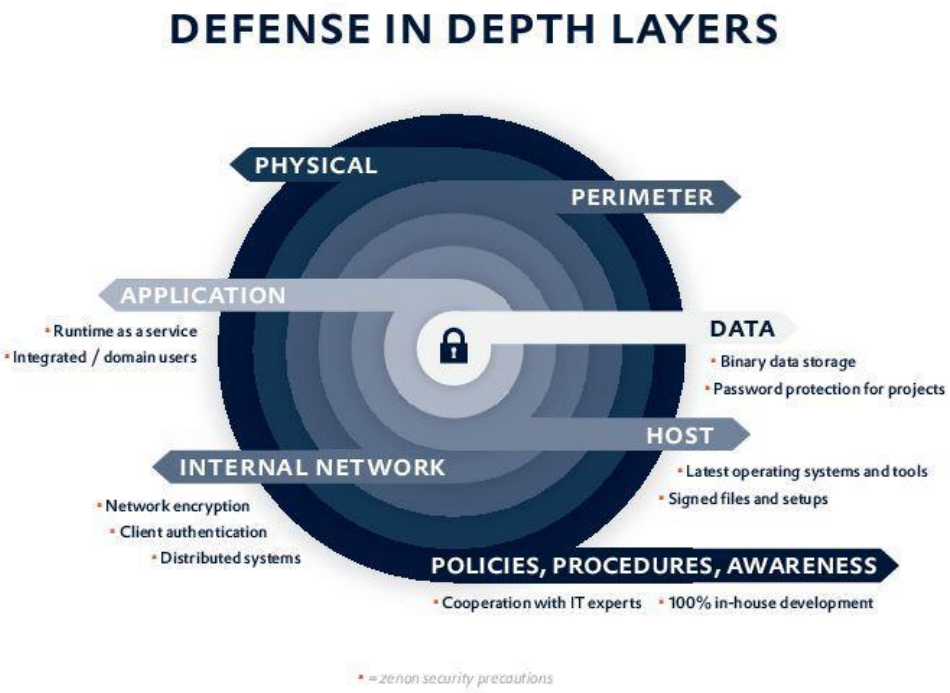
This ensures attackers need to overcome a number of barriers before they get to the core of the production system. The overall strategy is topped off with open dialogue and documentation about security. A HMI/SCADA software provider should work closely with its customers to strengthen security guidelines and build on its industry experience.

5. Update and communicate

Knowledge and understanding of cyber security risks should not end with engineering and IT staff. In fact, according to respondents of the Global State of Information Security Survey 2016, the most cited source of security compromise lies with employees.

Internal security compromises may not be intentional, but could prove just as damaging as an external attack. To begin, organisations should consider how much the average employee actually knows about keeping industrial systems secure. This could be as simple as encouraging staff to use strong passwords, delete unwarranted e-mails and update computers regularly. These basic measures go beyond the IT and engineering departments and should include other departments; even senior management.

After a thorough assessment of the system's potential vulnerabilities, creating a procedure and then training members of staff on industrial security should be the next step. Larger organisations might find it helpful to appoint a Chief Information Security Officer to manage all industrial security issues and communicate the importance of cyber security, thus creating an engaged workforce and a company culture built on safety and security.



Industrial technology is evolving at an incredible rate. While upcoming trends such as cloud computing, IIoT and big data are certainly beneficial for the manufacturing industry, they also generate entirely new challenges for those managing the industrial security and data protection of organisations.

The days of Stuxnet may be behind us, but pharmaceutical manufacturers need to stay ahead of the industrial security game if they want to avoid security breaches and the negative consequences they entail. The best way of doing this is by working with experienced, reliable partners that understand your industry and are leading the way in cyber security.