Radiflow

Securing Pharmaceuticals from OT Cyber Attacks

June 2022

1. Introduction

Pharma companies discover, develop and manufacture both medication and medical equipment that range across Vaccines, Prescription and Over the Counter (OTC) medications. Many of these products are critical to either sustain life or cure illnesses.

Like all companies that run computer systems, they are not immune to cyberattack and in recent years, the industry is seeing an increase in debilitating attacks on both traditional IT systems and more recently Industrial Automation and Control Systems (Operational Technology [OT]), used typically across R&D, Manufacturing and Warehouses. These attacks have the potential to halt both the discovery and production of medication and may lead to a lack of supply of patient critical mediation or devices.

In 2017 the industry was impacted by a wide spread notPetya “ransomware” attack that effected many business’ including an overarching impact across Merck’s corporate and manufacturing environment which took months to recover from and resulted in an insurance claim of $1.4Bn.

Within Pharma, the OT environment is typically more fragmented than traditional IT, with many instances of systems and machines, driven by the number of factories, warehouse or R&D facilities and the need for fast local processing (network performance). The focus in OT has traditionally been around safety, quality, performance (OEE), and longevity of the asset and less about Cybersecurity hygiene.

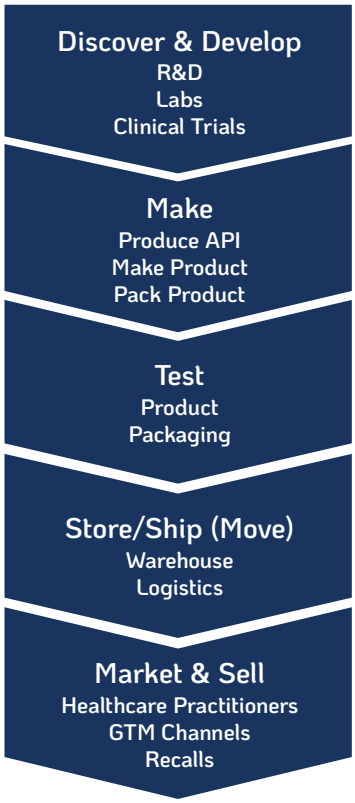
Historically shop floor and lab systems where built to run independently / standalone and detached from the broader corporate intranet and internet. As Pharma’s digital ambition has grown and with regulatory drivers, more and more OT systems are being connected, internally to enterprise systems, like ERP, Lab and Quality and externally to third parties.

This in turn is providing benefits in building a smarter factory with considerable savings and quality improvement opportunities in key areas such as moving from a paper Batch Record to an Electronic Batch Record System and being able to “release product by exception’ through having robust data that meets ALCOA data integrity principles.

2. The Pharma Process and its OT Touch Points

Pharma processes span from R&D to Make, Test, Move, Market and Sell. In many of these stages whilst enterprise systems are leveraged there are many occurrences of OT systems that span areas such as Environment Controls, Building Management, Laboratory testing, sample management, warehouse management (goods in / goods out), production; control systems, process automation, weigh and dispense, packing, palletisation and so on.

The Pharma Process

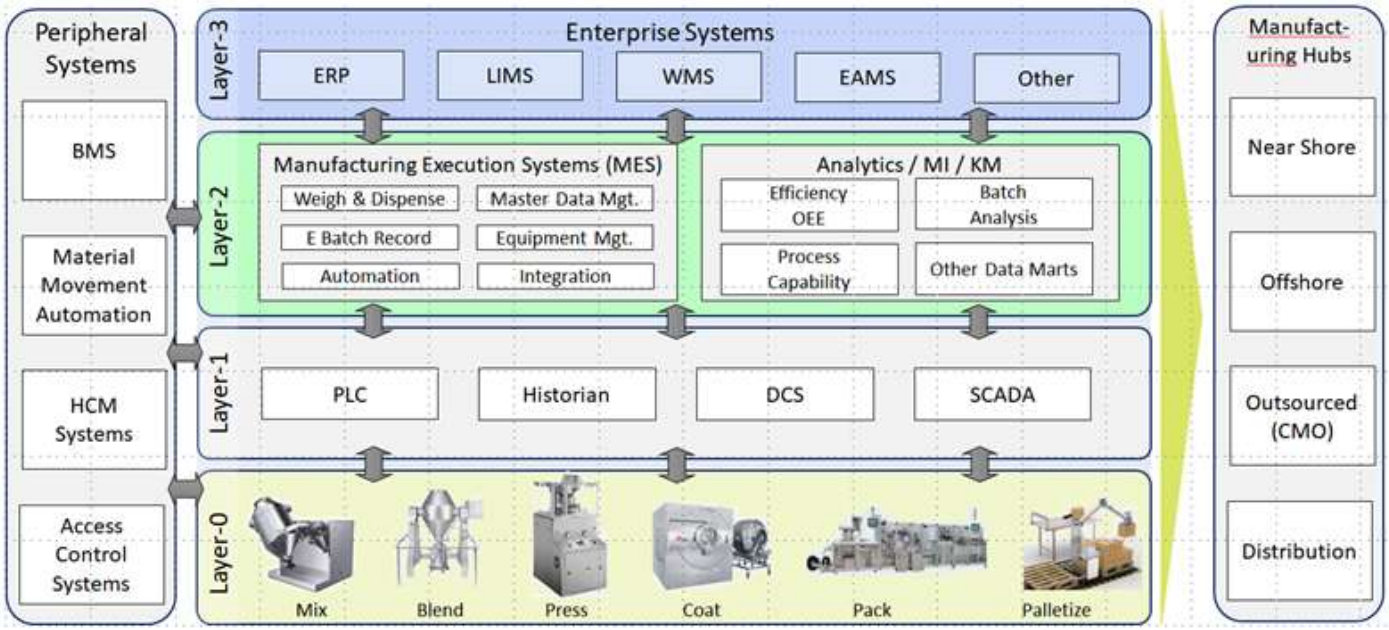


With the world of Digital, IOT and IIOT we're starting to see more and more connected technology spreading in the supply chain (Serialisation, Track and Trace, Temperature tracking ....) and also into the consumer with an exploding potential of wearables and mechanisms to monitor and control the medication taken.

As the modern day digital agenda unfolds, across the application and systems landscape connections exist across corporate intranet, OT networks and external network connections into OT operating environment. Network controls and monitoring are essential to manage this ecosystem from Cybersecurity related exposure.

The diagram below shows a typical manufacturing architecture in Pharma, where enterprise systems have broad connectivity, sometimes right down to the lower layers of the architecture.

For example, label printing or sending Bill of Materials information to SCADA systems. Horizontally we see systems talking to systems as well as external network connections to other company locations or third parties. Third parties providing CMO or CRO (R&D) capabilities as well as potential equipment maintenance and monitoring back into a factory. As such, a modern day factory requires a level of connectivity both within and external to the site that increases the risk of bad actors or Malware infection.



3. Risk Management and Solutions

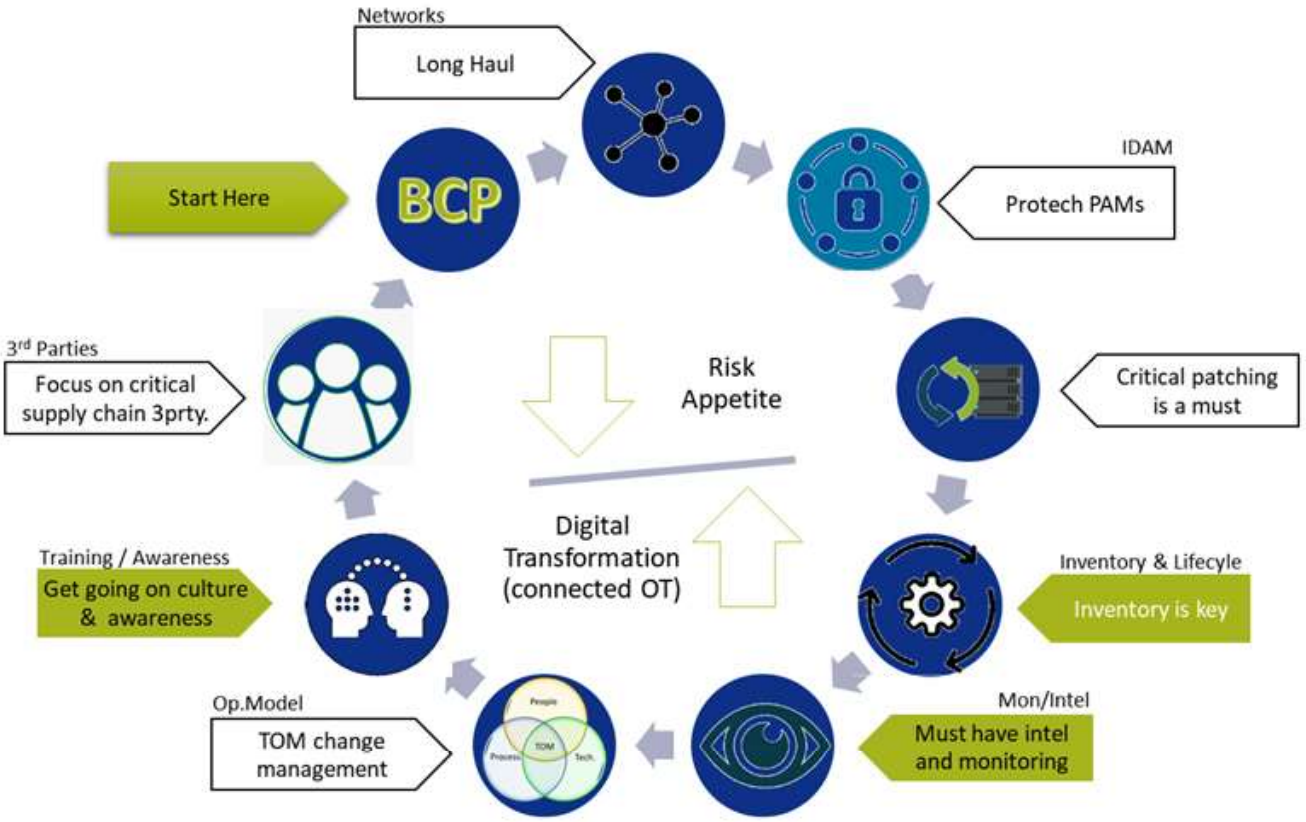
Frameworks such as the NIST Cybersecurity Framework and the IEC62443 Standards serves as a pointed reminder to manufacturing companies and other providers of critical infrastructure that securing the ICS should be made a top priority and systematically addressed before irreversible consequences are suffered.

The NIST framework provides guidance on standards, guidelines and practises for organisations to tailor and adopt as required by their risk tolerance. NIST recommends commencing with an "information security risk assessment" to identify threats and vulnerabilities, the harm they might cause, and the likelihood to occur at the organization level, mission/business process level, and information system level (IT and ICS).

As a starting point, companies must first recognise where they are in their journey to establishing OT Cybersecurity Risk Management and Remediation in an organisation. One of the he first steps is to be able to see what you have and know the current risk position for each OT / ICS asset, such that risk remediation can be assessed and prioritised by critical systems, or if you prefer, "protecting the Crown Jewels".

The following is an example "solutions" framework that may be applied in establishing an OT Security Program. Each solution can be considered to have merits of reducing the risk posture in an OT environment. Some are "just do it" solutions that can be quick wins or essential to a program of work.

The Solution Framework



3.1 Where to Start?

Typically it is the CISO of a company that is accountable for computer systems, data and sometimes physical security. However a program that impacts OT requires joint sponsorship of both the CISO and a business leader from the operating environment. In addition to implementing a program of solutions to reduce the OT Cybersecurity risk, leaders should work on a joint strategy and governance plan for the program.

The first step in a program is to understand business critical facilities and products. Business Continuity Plans, offer rich insight to an OT security program in providing a true business view of the criticality of a site to the business. These in turn, may warrant being modified and tested against a Cybersecurity breach.

Inventory and Risk Discovery. The next step is to undertake an initial risk assessment of the OT operating environment. This requires discovering and cataloguing the OT assets and systems, undertaking a vulnerability assessment to establish current risk posture which in turn should be translated into key business risks. E.g. “this critical product / site / business process has a high risk score and probability which could result in the impact of the loss of £x revenue.

Assessment may be undertaken manually, however these will be out of date in days. Leveraging tooling will improve speed, accuracy and currency of the assessment as the risk landscape changes over time, as well as providing business prioritised risk views.

Training and Awareness: many organisations carry out “phishing” type training and awareness as part of a corporate program. Expanding this to help shop floor, R&D and Lab staff understand the broader risks in an OT environment, such as the risk of using a USB drive to apply updates can bring significant risk reduction. A large percentage (60%+) of Malware is introduced by Staff.

Security Monitoring ideally should be established to be near real time to recognise the changing threat landscape through either internal changes (such as new equipment being connected) or external threat intelligence showing up a new threat, possibly by geography or a new malware. These should be flagged and prioritised by business critical systems, most likely to be manufacturing lines, distribution centres or R&D labs. Additionally third party access should be monitored for unusual activity.

Network Segmentation is one of the key solutions that organisations may start with. There is no doubt that it brings value at either site level or value stream (product) level in increasing security controls and potentially enabling a zone to be cut off quickly as needed. Segmentation takes time and can be expensive, as such time to value may be years in a larger organisation.

Identity and Access Management (IDAM): the notPetya malware leveraged privilege access to rapidly gain access and cause damage to many servers and PCs. Privileged Access Management in particular should be tightly controlled and use of a single enterprise master privileged account must be avoided at all costs. IDAM tooling should be explored to check out / check in and audit of PAMs accounts.

Additional consideration should also be given to leverage digital invitation on the shop floor, like BioMetric bands as this makes it much easier for a gowned, masked and glove operator to log in and log out of a system, vs leaving accounts logged on and unattended.

3.2 Third Parties

The reliance of third parties, either locally or remotely is embedded into the modern day business ecosystem. With third parties being allowed on-site or remote network connectivity, controls should be applied to reduce the risk of malware or remote attack being introduced. Controls such as USB stick scanning and potentially scanning any IT (laptop) brought on site should be implemented as well remote connection monitoring. Some companies apply "open time" windows to limit remote network access.

Where external third parties are used, such as contract manufacturing [CMO], contract research organisations [CRO], supply chains and maintenance, it is important to know that they have good cyber hygiene and controls in particular when handing sensitive data. A third party security assessment approach should be leveraged as a minimum to measure and track the level of maturity in those organisations Cyber Hygiene. This is a complex and growing area in the industry where potentially a crowd sourcing approach may work well, i.e. one company assesses and shares.

Critical Patching. Within the IT environment, the culture and discipline of critical patching for new security vulnerabilities are robust and mature. In OT, this is a recent change in both culture and practise, with shop floor staff and labs typically focused on quality, safety, performance and sustaining expensive aging assets. Where systems can be patched, and the vendors even provide timely updates, this often has challenges in just securing the operational down time. As such organisations must build both capability and embed critical patching into standard work in the manufacturing, lab and R&D environments. Clarification of accountability should be factored into and OT Security Operating Model. Critical patching should be prioritised by threat likelihood and critical systems.

Where systems just can't be patched, then additional controls leveraging such as network segmentation and DMZ should be considered.

Target Operating Model: A key step in establishing a sustainable cyber secure OT environment is to address the gap between IT / OT language and understanding of way of working and priorities. Often this is as simple as building relations ships and starting to understand different drivers in standard work. Once a program is establish, a key step towards maturity is developing a target OT Security Operating Model. This will address:

- *Accountabilities*: Who owns, runs and maintains (including lifecycle management) the technology in the OT environment?
- *Standards:* Which security standards shall be adopted when buying / building new or upgrading key OT assets?
- *Process:* Who does what when a Cybersecurity event occurs? (Incident / Recovery etc)
- *Management Monitoring and Control:* Who monitors and audits the environment for Cybersecurity compliance to standard and process?
- *Partners:* Considerations should be given to the role of partners in both System Integrators and external SOC / SIEM capabilities to ensure they are a the right level to support the operating model.

3.3 Overarching Approach

Whilst there are many solutions that can be applied, the first step is to just start. Security C-Level understanding and a program of work jointly sponsored by CISO / IT and Business Leader is key. Thereafter having visibility of risks, in particular for crown jewels (business critical products / sites / process) and then establishing a joint Strategy and Governance approach to secure funding. Potential some initial pre-funding may be required to establish risks and priorities. Operating Models and Internal OT Security Standards can be developed on the journey to maturity. Industry standards and guidance such as the NIST Cyber Framework and IEC62443 should be adopted as appropriate for the organisation (unless regulated when they must be adopted) and will provide additional structure to enable leadership and good practise.

4. Radiflow's Solutions for Protecting Pharma OT Systems

Leveraging technology for discovery and risk management of OT connected systems and devices can both accelerate an organisations understanding of their risk posture and provide ongoing and near real time visibility to a changing internal and external threat landscape.

Radiflow's OT-security solutions, which have been successfully implemented in a number of major organisations worldwide, bring industry excellence in the discovery and risk management of OT at enterprise level with additional industry leading value from enterprise risk visibility, laser focused reporting and planning by critical assets. These products enable CISOs to quantify and prioritise risk and impact in ways that business owners will understand and jointly support funding proposals.

Radiflow's multi-prong solution provides anomaly detection and threat monitoring on the OT part of the Pharma infrastructure (R&D, Labs, Manufacturing, Warehouse and Distribution) to ensure the detection of breach attempts originating from the IT network. The Radiflow solution further improves network oversight by providing full visibility (via network "maps") into the OT network, including all and device properties, vulnerabilities, communication protocols and possible intra-network attack vectors.

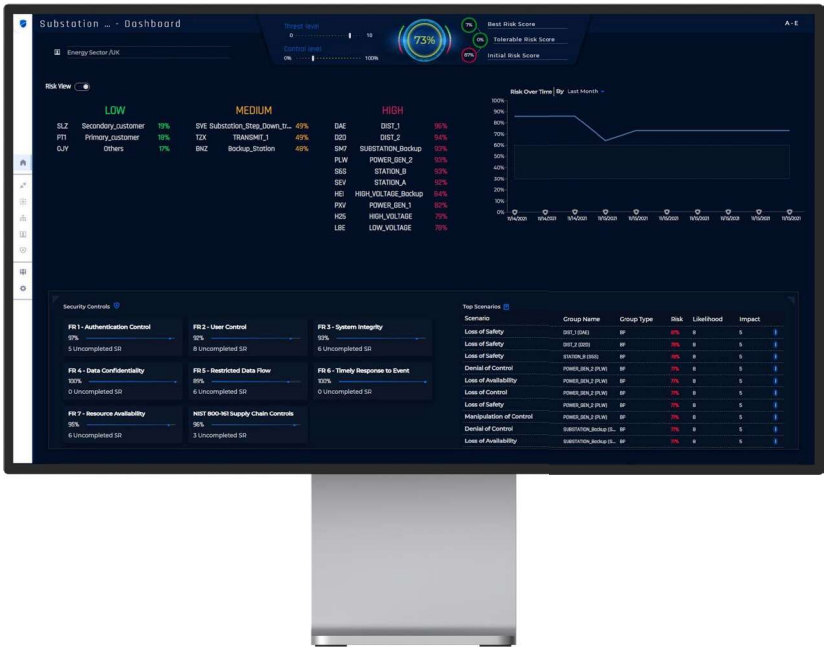
Once discovered, assets are grouped into Zones (connected by Conduits) to facilitate IEC 62443-compliant risk assessment & management.

Using multiple data feeds for newly-discovered threats and vulnerabilities, as well as rich contextual information received from equipment vendors for cybersecurity analysis, Radiflow's threat detection and monitoring solution provides operators full control over anomaly alerting and incident handling.

Going beyond threat detection, network visibility and security assessment, Radiflow's risk management platform empowers users to optimize their cybersecurity expenditure by prioritizing the threats that pose the most risk to the organization as a whole (accounting for the impact of a debilitating attack on each zone/business unit or critical asset) and subsequently the mitigation measures best suited to reducing the most risk and thus increasing the ROI of the entire cybersecurity operation.

Radiflow's risk assessment process involves analysing thousands of network data points and asset properties, threat intelligence and impact calculation to provide various KPIs and full reports for the network's risk state:

- Network and asset properties: using non-intrusive self-learning of the OT network, Radiflow creates a complete digital image of the network with all network, communications and assets properties and vulnerabilities. The digital image serves as the baseline activity model for assessing risk and OT cybersecurity planning.
- Threat intelligence: newly-detected threats and threat players' capabilities are analysed and published by a number of dedicated agencies (e.g. MITRE ATT&CK) as well as by others, including Radiflow's own research.
- Zone impact & criticality, risk tolerance and other considerations: assets and business processes are grouped into zones with different levels of criticality and security needs.



Radiflow's CIARA OT Risk Assessment & Management Platform analyzes thousands of data points for network and asset properties, threat intelligence and impact calculation, toward providing various KPIs and full reports for the network's risk state.

All asset, network, threat and SuC owner-provided data points are used to run numerous non-intrusive breach and attack simulations.

The simulations determine the most impactful threats to the network and subsequently the most effective mitigation controls that deliver the most risk reduction per dollar spent.

The results of Radiflow's risk assessment are provided in the form of various high-level and detailed reports used for budgeting, auditing and follow up, as well as a detailed mitigation plan listing the most effective (high-ROI) mitigation measures, accounting for the user's budget and risk management preferences.

In Pharma, Radiflow solutions will enable cybersecurity continuous risk visibility, management and reduction across business processes at enterprise and individual system level.

5. Conclusion

The Pharma industry runs a broad set of OT and IT Systems. IT systems, by process and vendors lend them self to a stronger Cyber Security ecosystem and in most cases be rapidly updated to meet existing in emerging vulnerabilities and threats.

Within the Pharma OT environments, the industry is are becoming more aware, however with the nature of ageing systems and the lag in OT Vendors Cyber Security by design it is essential to for companies to have a clear visibility of their OT environment, with a risk management and monitoring ethos that brings laser focus to critical business systems, locations and processes in order to call to action risk remediation.

The OT environment is typically more fragmented where there may be many instances of systems and machines driven by the number of factories, warehouse or R&D facilities and the need for fast local processing. The focus in OT has traditionally been around safety, quality, performance (OEE) and longevity of the asset.

The drive to connect more OT from either regulation or digital ambition and combined with the acceleration of the forth industrial revolution dictates that a pharma business must embed cybersecurity into their culture and standard work with OT and IT staff talking the same language.

An OT Cybersecurity program brings with it many areas to focus; the key to success includes shared ownership from top of the house (not just the CISO) and knowing where to start. A key first step in that journey is to be able to SEE what you have, KNOW what the risks are (especially for critical business process, locations or products), ACT on remediation plans to reduce risk and to continuously MONITOR what you have for both internal change and emerging external threats.

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 7000 sites around the globe.