Improving cybersecurity and data integrity

As drug manufacturing plants become increasingly digital and interconnected, their approaches to protecting their plant and data require cross-industry alignment to manage the risks and provide sufficient resiliency from external threats. BioPhorum Information Technology (BPIT) is tackling both complex topics.

MALCOLM CASEY
EXECUTIVE DIRECTOR
MANUFACTURING IT
MERCK & CO INC,
KENILWORTH NJ

> NO ONE COMPANY IN AND OF ITSELF CAN OVERCOME THE CHALLENGES THAT WE FACE AS AN INDUSTRY AND WE NEED TO CONSIDER THE WAYS IN WHICH WE CAN MOVE THE OVERALL BIO-PHARMA ECOSYSTEM FORWARD.

Cybersecurity

Cybersecurity is a key focus across the industry. The complexity of protecting digital plants from online threats is more than one company can manage alone. BPIT is developing a resilience model so that companies can ensure they are working towards best practice and that will, in turn, strengthen plant resiliency across the industry.

Malcolm Casey, Executive Director of Manufacturing IT, Merck & Co. Inc. has been involved with BPIT for the past three years and has been instrumental in the Cybersecurity workstream since its launch in November 2017. Casey explains the problems faced by the industry from cybersecurity threats to digital plants and how BPIT is providing the vehicle to create the alignment needed for better protection for companies and patients.

"Cybersecurity is a strategic topic that is relevant to all companies, so it is clear there is mutual benefit in discussing best practices, looking at the industry norms and how we can define and improve them. No one company in and of itself can overcome the challenges that we face as an industry and we need to consider the ways in which we can move the overall bio-pharma ecosystem forward. That includes not just BioPhorum members but also our suppliers and partners because we all must raise our game to address the ever-increasing risks. This is a topic that will benefit tremendously from collaboration in an uncompetitive manner rather than individual companies trying to address this challenge themselves because that will lead to sub-optimal solutions across the industry."

Casey highlights the benefits of being part of the BPIT community when looking at protection from cybersecurity threats and the recovery speed after an event.

"Merck & Co. Inc. is constantly working to improve the resilience of our manufacturing network and supply chain. We would like to understand industry best practice, and then leverage from others who face similar challenges. We also see opportunities to work in partnership with a group of companies, so that we can quickly define standards that will help our suppliers to tailor solutions that will address the ever-evolving cyber-threats.

"When we look at a cyber threat, the mechanisms and motivation of the attacks are continuing to grow. Tomorrow's threats will not necessarily be known today, so leveraging the collective wisdom of the group will help to protect the industry and most importantly, help to ensure the continued supply of medicine to our patients – that is the overall goal of our industry. Additionally, there are a lot of dependencies across companies through joint ventures and supply chain dependencies: such as the provision of active ingredients between companies or contract manufacturing relationships."

The problems faced by the industry have a scale and depth that is challenging even within a collaboration, but it is the strength of working together that provides the greatest protection. This is true both in terms of 'herd protection' but also in setting the expectation levels about what can be achieved, so that members can invest in the right areas.

As Casey explained: "One of the first things that we want to do with the resilience paper is to set realistic business expectations in relation to the investments required and the defined business outcomes. That will be key and it is lacking in the industry at the moment. The development of an industry standard model can do that for us and it will also enable us to have a common understanding of the topic and have common terms in relation to how we define both the problem and the opportunities. It will also provide a sequence of steps for how we can move from where the industry is today to where we need to get to.

"BPIT offers a unique platform to undertake this collaborative work as they are focused specifically on manufacturing networks. In manufacturing, we generally deal with technology platforms which change on a much longer life cycle than in the other parts of our companies. Developing a best practice approach for addressing cyber-threats in a manufacturing environment is a specific challenge, particularly when you are dealing with threats that are continuing to occur at an increased pace. This requires the Manufacturing IT teams to come up with novel approaches as to how we can protect our companies but also recover quickly in the event that there is a scenario where we do have a breach."

Data integrity

The Data Integrity (DI) paper released by BPIT in 2017 focuses on how to protect data from risks and comply with regulatory requirements. The best practice guide provides a common industry response for regulators and will increase the confidence in companies' approach to compliance.

The guidance outlines the controls required generally and those required specifically for three categories of IT systems – enterprise applications, local systems and equipment.

The paper describes the IT systems and equipment impacted by the data integrity guidelines, inherent risks, the controls required and industry best practices from an IT perspective. Data integrity has been a focal point for regulatory agencies worldwide in recent years and is a key aspect of inspections, including the focus on good clinical practice, good manufacturing practice and quality. Data integrity is critical because a lack of integrity undermines the assurance and confidence in drug safety, efficacy and quality.

Currently, there is no one-size-fits-all solution to ensure compliance with regulations across the entire data lifecycle and systems landscape. Understanding data utilization, the strengths and limitations of systems and then leveraging the available technology to manage gaps are all key to moving towards a compliant position.