VERVE

BEST PRACTICES:

IN PHARMA/MEDICAL DEVICE MANUFACTURING CYBER SECURITY

Introduction

Cyber security in operational technology (OT) is a challenge in almost any industry. The combination of devices aging, embedded proprietary software, 24x7 operations, etc. makes managing security a difficult task.

In pharmaceuticals and medical device manufacturing, those challenges are exacerbated by regulatory burdens and risks to patient safety and personal information in some cases. The pharma/med device CISO's job is a difficult one.

The good news is that there are ways through this minefield with proper planning, procedures, and technology. This document lays out some best practices for pharmaceutical and medical device companies based on our own work and research in the cyber security field.

The Challenge

If you are reading this, you are likely only all-too-familiar with the challenges of cyber security in medical device and pharmaceuticals. We categorize them into three areas:

- The Systems: OT systems in pharmaceuticals and medical devices closely resemble those in other manufacturing environments with several specific and important differences.

  These OT systems contain many of the proprietary embedded devices commonly found in industrial manufacturing of different forms. PLCs, panel-view monitors, HMIs running proprietary control system software all exist within these plants. These systems are often old and designed to operate with PLC firmware or HMI OS that is out-of-date and no longer supported. These systems are sensitive to improper communications which make using many IT-tools risky to the reliability of the devices.

  These systems are usually networked to provide access to OEM partners for trouble-shooting as well as corporate applications for analyzing inputs and quality outputs.

But beyond the traditional OT system challenges, pharma/med device environments have additional unique challenges:

- **Integration with lab and testing equipment in the same facility.** These devices offer their own challenges to secure given their operating systems and the information they control.
- **Potential presence of patient personal information.** In most manufacturing environments, while information is important from a competitive point of view, they do not host sensitive personal information of customers. In many modern pharmaceutical and medical device manufacturing, specific customer information is fed into the manufacturing process.
- **Internally designed control systems.** For many operators, the actual machines themselves constitute important intellectual property. These control systems were often developed ten to thirty years ago without the same documentation or change management as you might find in commercial systems.

- The Regulations: Almost every industrial sector operates within some regulatory boundaries. But pharmaceuticals and medical device manufacturing have the most significant restrictions. Here's how we've seen these regulations challenge traditional IT (or even OT) security practices:
  - **Changes to validated systems.**¥\éÇ¥ïÐ¥ąÕÇ¥¾ïüÇ¥ē²ęÃ¥ïÐ¥üÇÃĉ¾xéÑ¥ü×Āà¥×é¥è ÇÃ×¾²â¥è²éĉÐ²¾ąĉü×éÑ¥×Ã¥ą ï¥üÇÃąü×¾ą¥¾Õ²éÑÇÃ¥²éÃ¥ÇéĀĉüÇ detailed testing and documentation of any changes that do occur. Even though one of the tenants of cyber security is to monitor and reduce unintended changes, proper security requires updates and changes to systems on a relatively frequent basis - to update anti-virus signatures, deploy security patches, update older PLC or controls hardware, etc. This is both a technical change (confirming patches will not result in inappropriate changes to the process) and a procedural change (conducting the paperwork and process elements necessary to comply with the regulatory requirements).
  - **Ensuring process data is stored and analyzed.** To ensure quality and consistency, regulations require that manufacturers monitor outputs and testing, as well as process levels and readings. This requires that the data flow across the network enables analysis and storage. In many cases, these analytical systems are stored in corporate IT data centers, adding extra challenges to network segmentation, access control, etc.

- **Historical procedures.** Regulations limit technical processes and control systems changes, and also limit changes to the underlying procedures pharmaceutical and medial device companies use to manage those systems. In many cases, change control procedures and the systems used may differ by plant due to the various geographic differences or prior ownership decisions. Consistency of procedures is a hallmark of cyber security success so the whole organization operates in a coordinated way. These historical procedural differences can cause delays and barriers when aligning corporate-wide processes.

- The Organization: There are always organizational challenges to OT cyber security: ownership of the systems between corporate IT, Plant IT, CISO, engineering, etc.; responsibility for OT systems management; lack of budget alignment; limited staff at the plant level that understand cyber security policies or technical actions, etc.

  In addition to these already challenging organizational dynamics, pharmaceutical and medical devices manufacturers face a few more:

  - OT systems groups are owned by different organizational departments - manufacturing, labs, building controls, networking, and plant personnel - IT may be owned by different parts of the organization, creating alignment challenges.
  - Regulatory change management organization has a very strong role in any decision-making.
  - Internal control system/manufacturing equipment development means there are often internal development groups to manage.

While all of these challenges exist to some extent in other industries, their presence in pharmaceuticals make the OT cyber challenge even more complex.

The Framework

Over the past several years, Verve has built a set of best practices and approaches to address the cyber security challenges in various industries. From our work and research, we developed a framework of four best practices that form a roadmap for successful cyber security in manufacturing.

- **Leadership alignment.** More than in any other manufacturing environment, alignment among senior leadership is absolutely critical within pharmaceutical/ medical devices. The above challenges mean that the necessary changes will require buy-in from a wide range of stakeholders, cross-functional coordination, personnel commitment and training, budget alignment, etc.
  Key areas of alignment include:
  - Largest areas of risk
  - Responsibilities and ownership of key decisions
  - Roadmap and timing
  - Budgets and authority
  - Objectives (metrics/ security standards/ milestones)
  - Ownership of ongoing maintenance and audit
- **Robust assessment.** To gain proper alignment, the organization requires a data-driven assessment of risk and vulnerabilities that is then transformed into a specific security roadmap. One of the challenges in many OT environments is mistaken assumptions about the current risk or vulnerability situation: “we have firewalls, so the network is secure”, “we regularly patch IT systems, so OT systems are likely patched as well”, “we use Active Directory, so users access control is limited”, etc. Although the design may be great on paper, the reality of specific network devices configurations, network connections, software present on systems, etc. is a different matter. Things drift from the standard or the ideal design. A proper, asset-by-asset assessment covering what “is”, not just what “should have been” is critical to enabling clarity of the actions necessary to secure the environment.
- **Integrated roadmap**. Once the assessment is complete, the organization can build a “portfolio of initiatives” or sequence of actions to achieve the desired level of security across the environment. This roadmap provides clarity to budgeting and resourcing of the initiatives.

The roadmap needs to include:

- Sequencing of initiatives: This is critical as there as components that need to be completed in advance of others
- Operational awareness: Identifying when and how to execute remediation based on production schedules is key. With the proper policies and planning in place, this can be done with little or no interruption.
- Assessing total cost of ownership: Too often, budgets do not consider the human resources to maintain the security once deployed.
- Audit procedures and tools to ensure that targets can be assessed on an ongoing basis to demonstrate success and gaps.

- **Apply "balanced scorecards" across the functional groups.** To deliver on the roadmap requires close coordination among many groups within pharmaceutical/medical device companies. Compliance, Plant IT, CISO, infrastructure/networking, engineering, finance, HR and perhaps other parts of the organization have a role to play. Organizations have many cross-functional requirements: safety, environmental, and others. Cyber security can be approached in a similar fashion.

  These programs have a history of success. Each organization approaches them differently, but in most cases, these elements become part of the "balanced scorecard" of key line managers. There is a central team whose role is both to help establish policies and procedures, as well as provide subject matter expertise. Critical to this is creating metrics and standards that are measurable. These should be included in each functional area's balanced scorecard.

The Specifics

How do you generate alignment at the top?

Obviously, this heavily depends on the organizational dynamics. While these suggestions have practical results, each organization requires its own specific approach. The key challenges we see include: delay due to debate over "what good looks like", delay and confusion due to ownership of key decision-rights, budgeting and resource alignment, etc. Several key learnings we have discovered in our research and experience have helped.

- **CISO led, but team aligned.** The role of the CISO is key in leading the team to the right posture and strategy. yber security can be very difficult to communicate to senior leaders with little exposure to the challenges. The increasing number of events within manufacturing environments is certainly raising awareness. But the details and implications require explanation and simple communication. The CISO is normally the person in the organization best placed to bring that level of clarity.

  At the same time, the CISO cannot act independently. He or she will need to work closely with the CIO/Plant IT Leadership/Engineering/Finance and other senior team members to create alignment and to understand the implications on each part of the organization.

- **Leverage the CIS Top 20 Security Controls and their recommended maturity guidelines as a starting point.** Many companies begin with a focus on the NIST Cyber Security Framework or ISO 27000. Both of these standards provide overall direction and procedural steps. They do not resolve, however, the biggest challenge we have seen – i.e. defining what "good looks like" within each control area. Cyber security is a complicated topic and many organizations spend a significant amount of time trying to build their NIST CSF profiles and tiers.

  The CIS Top 20 Controls offer a starting point with a set of rigorous guidelines for each sub-control. Instead of starting with a blank piece of papers, the CSC20 offers an initial basis from which to work. The guidelines are not going to be perfect for every environment or every asset. But they allow an organization to edit, rather than create. We have found this to streamline the process dramatically.

- **Identify the ends, not the means.** We often find that lengthy debates happen among senior teams trying to align on exactly how OT should secure itself. The security team believes OT should use the same tools as IT does. IT admins argue that they cannot manage these end points without the same procedures as IT devices. We have seen the most success where the senior team establishes a clear objective (using something like CIS CSC20 or other guidelines) as the objective, or ends, of the program, with clear and measurable targets. They then leave the "means" or the specifics of tools, resources, etc. to the team responsible. Sometimes this leads to less apparent "efficiency", but leads to much faster time to detection and remediation. And, in fact, the inefficiency is much less than some would fear.

- **Speak the language of the CFO.** One of the major stumbling blocks in cyber security is defining an appropriate budget. Successful CISO's learn the language of their particular CFO/financial organization and develop robust business cases for that audience. No two large organizations' finances are the same. Although all finance departments balance across all elements of a balance sheet and P&L, the key metrics that drive decisions may differ. Some focus on headcount, others on capital expenses, and others on operating expenses. A CISO must understand budgeting well enough to build a robust business case with the underlying elements of total cost of ownership and risk offset, and position it in such a way that addresses the key financial objectives of the organization.

- **Hold plant operations (or engineering) accountable.** This refers back to the notion of the balanced scorecard discussed earlier. It is key that operations is ultimately accountable for the security metrics of their facilities. Otherwise, the security and IT departments are pushing on a wall. Operations and engineering teams, rightfully, drive decision-making in pharmaceutical and medical device manufacturing. There are too many financial and manufacturing risks to have it any other way. To drive traction, the top team must add security to their balanced scorecard, forcing them to make the difficult decisions necessary around topics such as patching, replacing older equipment, segmentation designs, etc. The security team should be a very active participant, helping to shape the engineering and operations' teams thinking to offer solutions and guidelines. But the only way for a program to be sustainable is if operations adopts and absorbs it.

Who should "own" the cyber security program and what is the role of the security organization?

See the above point on plant operations/engineering. In short, we have seen most success when the operations team owns the deliverables. By the same token, the security team has a critical role to play. We see three key roles for the security team.

- They should be instrumental in developing the overall roadmap and senior team buy-in. They should aggressively drive the agenda and help drive agreement about the risk and expected guidelines.
- They should provide subject matter expertise and scale to the asset owners for specific areas of their domain expertise. This would include input on possible methods and tools for achieving security objectives, managing central security elements such as vulnerability and threat intel, and development of corporate procedures.
- They should act as the referee for the organization when it comes to measuring success against the overall scorecard or where questions of compensating controls are raised.

How do you achieve a robust vulnerability assessment without risking the sensitive OT systems?

- **Select the right representative environments.** We find that assessing 3-5 provides enough information to build an effective roadmap.
- **Leverage technology, not just manual assessment processes.** Too often, we see manual assessments (with sampling of data, manual asset inventories, review of sets of firewall rules, etc.) that are both too narrow and shallow as well as quickly become out-of-date after they are completed.

  A software-enabled solution allows you to see every endpoint, every piece of software, every firewall and switch ACL, etc. Further, it is constantly updated to ensure the assessment is up-to-date and has the ability to measure progress.

  Second, closely aligned with the first, the technology needs to be proven safe and effective to operate in OT systems. Vulnerability scanners, inventory scanners, some agent-based tools, etc. can either be ineffective or worse damaging to OT systems.

  Third, do not invest in expensive span ports and taps just to conduct an assessment. Assessment software can be done with no hardware required. Do not fall into the trap of the need for expensive deployments of PCAP capture. There is an alternative.

- **360-degree view of vulnerabilities.** Too often, we see companies focus on missing patches and configurations in their assessments. The key is to see across all elements of defense-in-depth: procedures, networking, access control, and endpoint vulnerabilities.
- **Ongoing/real-time assessment rather than one time.** One-time assessments are often out of date by the time they are completed. The assessments should include a way to monitor ongoing vulnerabilities, especially as security increases and new vulnerabilities are published.

To be fair, the above closely aligns with the Verve Security Center platform. We are not saying the above because our product does these things. We built our product because we believe these things.

How do you secure validated systems that cannot be patched or updated regularly?

We have seen a four-part model work for this in practice:

First, get a 360-degree understanding of each asset to understand the operational risk, actual patch status, configuration status, and potential for compensating controls. As one refines the scoping, the number of unpatchable critical vulnerabilities comes down significantly. You gain a fact-based perspective of the possibilities for compensating controls to protect between patch cycles.

Second, deploy compensating controls where feasible – and the most effective is application whitelisting. DHS analyzed all industrial controls events and discovered that a full 38% would have been stopped with properly configured application whitelisting. This is an under-used and particularly effective control in manufacturing systems where you do not want new applications to run. It requires a trained-hand to configure effectively and safely, but it is doable and incredibly effective. Other compensating controls might include additional segmentation protection, reduced access controls, etc.

Third, prioritize, prioritize, prioritize. Not every vulnerability is critical, and even those that are may not have exploits. If you do have compensating controls in place, narrow your focus to those most critical ones.

Finally, build a consistent test and change control process. One of the biggest challenges is that each plant may have its own change process and rules for testing. Corporate operations and engineering must work with IT to develop a consistent process – across plants that may have been acquired at different times – and across systems to build a testing process that all have faith in. This requires an investment upfront, but the ROI on such a centralized test and change process is less than a year.

How do you provide OEM or corporate IT access that may be necessary?

We have seen many instances where segmentation is well-intended, but over time changes have occurred in rules to enable various groups to access the manufacturing control systems for logical operational reasons: maintenance, analysis and troubleshooting, analysis of output data, etc. In many cases, firewall rules are put in, or worse, devices with dual NIC's are set up so that OEMs and others can access necessary systems without the need to go through the firewall. In many cases, we have seen LogMeIn and other remote access software on control system HMIs (before you scoff, you should check your own).

There are solutions that do allow for access when/where necessary but do so in a controlled fashion. To be clear, remote access is one of the riskiest elements of industrial control systems. Third parties may not have the same security as you do internally. You do not control their employees as you do your own. It requires careful limitations and monitoring. If it can be shut off all together, all the better.

However, in many cases, this is impractical. Solutions that require vendor access through a specific host managed with firewall settings, monitoring all behavior, limiting access only to necessary systems, automatically logging them out after a period of time, and, certainly, requiring robust personnel checks are ways of dealing with the possibly necessary risks of remote access.

How do you secure internally-developed systems from 10, 20 or 30 years ago?

These systems are usually critical to important manufacturing processes and really cannot be re-built on modern, secure platforms in a short period of time. We recommend a two-part approach:

First, protect them through separation and segmentation. Although we see the benefits of the push to Industry 4.0 and other connectivity elements, if these systems are critical to operations and use old code, the risks of connectivity may outweigh the benefits. Using data diodes or other highly secure network perimeters may be necessary. If not, sub-segmentation may be appropriate. If you have 10, 15 or 20 similar machines all running the older platform, segregate them into their own segment to ensure malware or access cannot easily hop from one to another.

Second, conduct a robust security assessment of the underlying software and system. When the assessment is completed, smaller changes are found that provide significant security benefit. Deploy other compensating controls such as application whitelisting directly on the endpoints. OT systems are tailor-made for application whitelisting. These changes do not solve all of the security issues, but allows significant increase in maturity without dramatic re-development of the software. This requires an in-depth code review and comparison of all the underlying components against known vulnerabilities.