Using **cyber security** to improve plant productivity

The domain of cyber security has traditionally been met by some Oil & Gas engineers with a mix of annoyance, suspicion, or even outright rejection. With production uptime taking the king of the hill position, any IT security equipment changes or modifications have ironically been considered as potential increasers of risk. Operations would rather isolate production from the rest of the company. IT, on the other hand, needs policy to protect the company assets enterprise-wide.

Among several advanced Oil & Gas operators is a new train of thought that recognizes the sheer necessity of leveraging new technologies – especially cyber security – to stay in business. Savvy plant managers are using cyber security initiatives as an ally in their drive to upgrade failing equipment, and to modernize plants to attain productivity, reliability and even safety benefits. Pragmatically, this often means opening connections into plant production. Instead of fighting this connectivity drive, operators are getting highly involved in their company's new technology choices in the cyber security domain, such as secure remote access controls, and helping guide toward solutions that bear their productivity needs in mind.

The timing could not be better, following the World Economic Forum recently reporting cyber attacks as the number three risk facing the world in 2018. There is a dire need to improve the industry's standing when it comes to cyber risk reduction, according to LNS Research -- only 37% of plants they surveyed are monitoring for suspicious behavior, and over half experienced security breaches in the prior year. Cyber security is the top technology challenge respondents face in deploying Industrial Internet of Things (IIOT) technology, and fourth overall when considering both business and technology challenges. As the LNS report indicates, "industrial companies woefully under-invest in industrial cyber security best practices across people, process, and technology, and survey results illustrate shortcomings in all of these areas."

By making industrial cyber security part of a larger modernization strategy, however, companies can not only build security capabilities into the business, but can also start improving overall plant metrics. Considering the board-level prioritization of cyber security (e.g. Equifax), and the growing industrial threat level (e.g. NotPetya), it makes sense for operational leaders to couple much-needed plant initiatives along with funded cyber security initiatives, rather than stopping or avoiding these efforts.

We have seen the following initiatives take place at customers in different regions, as examples of how to treat cyber security as friend, not foe.

OPERATIONAL CONTROL CENTERS

Many Oil & Gas sector initiatives cannot allow for additional resourcing, especially in dangerous or hard-to-reach locations. This has driven innovators in the sector to find methods that increase plant productivity while using the same or less level of resourcing.

Centralization of command centers and operational control rooms is one way companies are handling this need for greater efficiency, while at the same time using cyber security to improve productivity. Thanks to new technologies such as industrial secure remote access solutions and integrated industrial risk management tools, safe reach across multiple plants is far more attainable. Companies are locating staff with deep cyber security skills at a central headquarters, and servicing multiple plants, much in the same way corporate structures facilitate other roles such as finance, marketing or legal.

We are working with several customers to consolidate their control rooms, in some cases servicing dozens of plants globally, and in other cases, centralizing control centers within a particular region (e.g. Latin America).

The benefits of this approach include:

- Increased production & less downtime: As process experts spend more time together in a single location, we are noticing far greater levels of collaboration. Anomalies are more rapidly discussed, and the group insights are shared and applied, without having to overcome time zone or email procedure barriers. In some cases, through sheer observation of another expert performing their work, the other expert learns and applies new techniques.
- Less time spent on recruitment and training: With highly specialized experts available 24/7 centrally, there is less pressure on different plants to recruit and onboard cyber security specialists across disparate locations. Particularly in geographies where the job location itself is demanding, finding experienced cyber teams can literally take years. We repeatedly hear from customers, especially in the Middle East, that it's not just finding people, but training people that consumes significant team bandwidth.
- Increased staff retention: Hand-in-hand with less dependence on global recruitment, process control engineers deployed to more central locations report better job satisfaction. Instead of remote or even hostile locations, centralization efforts typically place control centers closer to cities and areas with richer social resources, for example.
- Modernizing plant operations: Most exciting for many of our operator customers, the same infrastructure developed for centralized cyber security can be used for many plant capabilities aligned with new Connected Plant concepts. These can include recording and checking online contractor sessions, to patching outdated software,

to performing various health checks and performance optimizations across the process control network. Once secure connectivity is in place, we are seeing more and more creative uses of the technology. Meanwhile, the tools themselves only continue to add useful operator features and capabilities, like drag-and-drop setting capabilities and intuitive data visualization.

OPERATIONAL EXPERTISE

As we move to more connected systems, the need for cyber security at the plant level is stronger than ever. Customers often mention their requirements to offload or lessen the burden on their plant staff, stripping away any additional responsibilities that are not focused on production and uptime. The LNS Research survey found that staffing for cyber security remains a significant issue. Approximately 45% of the responding companies still do not have an accountable leader for cyber security at the enterprise level, and 51% have no one leading cyber security for manufacturing.

For those plants with limited centralized staff options, or those who simply want to delegate cyber security management and liabilities, another productivity-enhancing trend is outsourcing. The Industrial Security Operations Center (SOC), can be fully, partially, or hybrid-managed, depending on the service level agreements or desired levels of support. In all cases, the reduction on in-house teams for managing security can significant impact daily productivity. Small teams bogged down by patching, can instead work on data analytics, for example, to find indicators to improve uptime or predict equipment issues ahead of failures.

We have a customer, for example, with a strategic priority to increase business agility, including the need for new exploration sites established within weeks. In their situation, the need to protect assets, people and operations could be better handled by highly trained, readily-available managed services teams, rather than by making the long-term investment to build an in-house security team. They may also use the managed service just for upstart, and then transition to teams if the exploration site shows promise.

The benefits of this approach include:

- Time-to-security-implementation: Skilled resources have highly specialized experience that limits how much time they require to adeptly "onboard." Combined with sophisticated risk management and remote access technical solutions, these teams can readily review, act on, and report on your situation with the right data at the right time. In contrast with building teams in-house, these service engagements do not require heavy processes (e.g. physical security clearance steps, travel approvals). What we hear from customers is often relief that they don't have to develop and build entire industrial cyber security teams from scratch, which they fear would slow timing and impact how many resources are left to focus on day-to-day tasks.
- Improved asset productivity: Paying someone to regularly review and update your assets consistently means you often gain more from your technology investments. We are seeing that even basic security management, such as industrial firewall rules tuning, improves system performance significantly. Specialized teams know how to correctly install the latest software, and perform ongoing optimizations, on a schedule that is set – unlike in-house staff with varied skills who "get to it when they can get to it," amidst dozens of other priorities. Using suppliers to service their own equipment further improves the speed and competency at which assets can be managed and protected. For your staff, not having to handle these tasks can increase their productivity, not to mention positively impacting their job retention and satisfaction.
- Knowledge transfer: As in-house staff work regularly with cyber security experts, they themselves gain a different perspective and risk reduction routine, which makes it easier to understand and act on security needs. Some providers (such as Honeywell) will include formal knowledge transfer as part of service engagements. This provides flexibility, in that you can turn in-house teams back on after a set period. It also improves productivity, since the learning for your people is hands-on and directly applicable to your unique configuration. In addition, we have seen that in-house staff appreciate the objective benchmarks and standardized data that providers can share, which is not knowledge they can readily find anywhere.

COMPETITIVE ADVANTAGE

Pushing for better plant productivity is ultimately geared toward competing better

globally, and winning more and longer-term business. As you develop your cyber security approach, consider how to leverage existing knowledge across multiple teams, including tapping into IT leaders, operational leaders, and engineering leaders. While this might seem daunting or even unpalatable at first (company politics?), any strategic initiative moving forward (Industry 4.0, Connected Plant) will at some point require it. As we noted, it's also no longer a question of if you should work together, but when and how. Competitive pressures are making some global Oil & Gas providers obsolete, while disruptors from different sectors are ready to pounce on inefficiencies in mature markets.

Taking steps now will differentiate your leadership and help staff evolve to develop the necessary new skills coming their way. Overall, the same teamwork and collaboration you develop for cybersecurity can help productivity, reliability and safety, and thus better differentiate. An easy method to categorize your steps is people, process, and technology streams, as we will describe further in a moment.

Our most advanced customers have one aspect in common – they have identified their industrial cyber security maturity level, and assembled teams as part of an Industrial Cyber Security Program, with defined objectives to reduce risk. What risk? More and more, what might have been a cyber IT risk is in fact, a physical operational risk. What might have been isolated threats in the past (virus on business network) are increasingly using multiple threat vectors (virus on USBs at control stations) and several steps (social engineering plant workers and email phishing). This is why it's critical to evolve your organization to better align with the sophisticated level of threat.

As part of their Industrial Cyber Security Programs, customers consider people, process and technology, and blend solutions to address the greatest risks. Companies with new staff, for example, invest in threat awareness to teach employees (people) never to use USBs they "found" outside their office or at a tradeshow. Companies that never had remote connectivity, as a different example, are now establishing policies to decide who can access the process control network, how, for what and how long (process).

Once again, making these programmatic moves for cyber security reasons will also deliver additional benefits.

- Better planning: Monitoring and measuring risks across both IT and OT makes it far easier to develop business cases and budgets for following year investments, whether people, process or technology related. We have seen more articulate and informed risk discussions once risk measurement tools are in place for several months, providing standardized, real data across plants, for example. In many cases, a risk area is outdated, long-untouched software (such as Windows XP), making the organization vulnerable. Viewing all machines enterprise-wide is a far smarter approach than leaving production machines out of the count for modernization or multi-year upgrades. Why not budget an initiative to replace all Windows XP, prioritizing those that have the greatest impact to production as those to fix first?
- Deeper insights: As with any team, garnering vastly different perspectives can inform a more resilient position. What are IT security threat analysts seeing that could be useful for operational leaders to know (e.g. phishing attacks on refinery plant employees, or repeated USB infiltration into particular plant location)? What are operational leaders' greatest concerns over IT touching their equipment, and how can they be considered in the team charter and procedures? Connecting security-conscious people has even changed how some of our customers run their organizations. Some institute job rotation programs or cross-functional roles, based on the insights and benefits they derived from building their diverse security program teams.
- Greater efficiencies: Whether defined as greater efficiency or improved productivity, the fact that 5 people instead of 25 individuals will track down and share threat information eliminates staff run-around, should any threat suddenly impact your organization. Your defined team, with clear roles and objectives, can communicate promptly, and share accurate information to help any area of your enterprise. Risk management solutions can even algorithmically prioritize what to do first, where and how, to automate and simplify team communications. Advanced systems literally build in explicit directions for non-cyber personnel to readily take action.

Of course, your specific situation will vary depending on your business and where it fits in the sector. There is an even higher cyber security priority for those Oil & Gas companies with field-level equipment that could be impacted by malicious commands (e.g. integrated sucker rod pumps, blow-out preventers, furnace thermostats). It may not be fast enough to only work your requirements into corporate initiatives alone. In addition, you may want to overlay your own regular local risk assessments, for example, or pen testing, as extra precaution that it's not your field team that is the weakest link. In these cases, you may want to trade-off some short-term productivity to assess and tighten vulnerabilities, knowing it will later pay off by saving human injury, corporate reputation, or simply your job if your plant is hit.

Overall, understanding that some cyber security programs and measures can actually align to your plant productivity needs may help you in the long run. Based on what we are seeing with the most advanced industrial leaders and their approaches today, cyber security is viewed as a strategic initiative that will not only reduce risk, but will help justify equipment and plant modernization.

Author
Greg Maciel

Contact
Honeywell Process Solutions GmbH
Offenbach
+49 (0)69 / 80 64 0