Building an Operating Technology (OT) Cybersecurity Organization: The Lyondell/Basell Journey toward a More Secure Manufacturing Network

Michael Norris
LyondellBasell

Abstract

Business executives, regulators, customers and the general public now understand companieswith industrial facilities face significant cyber risk. In response, executives and boards are requiring improved Operating Technology (OT) cyber risk visibility to avoid safety and financialimpacts. They also want data that proves how an OT security program investments have reduced risk.

Several years ago, the LyondellBasell IT and OT security teams began shifting their approach from security management to risk management. The shift occurred to eliminate vulnerabilities on our networks. Over 10 years, the company has maintained focus and has continued drivingtoward improved security on all systems within the LyondellBasell domain. Most recently, the company has placed an increased focus on the OT systems security.

The focus of this paper will be to better understand how the shift from security management to risk management occurred at LyondellBasell. You will also hear how the OT security team adapted to meet new risk management-focused governance models, security standards and integration requirements. Some of the measurements for success will be shared and how thosemetrics provide enhanced visibility into process control network security. Lastly, the skillsets required to meet the needs of industrial OT security support will be addressed.

Introduction

Cybersecurity events increasingly affect companies and entire industries. Consequently, manufacturing companies realize cyber-attacks pose a significant risk, despite a history of never finding themselves as traditional targets. A single major attack can potentially bring any operating company to its knees.

In addition to the rising impact of cybersecurity incidents, the upward trend of digitalization (integrating Operating Technology systems with Information Technology systems) only increases the company's attack surface. Not surprisingly, executives and boards require improved insight into OT cybersecurity measures to avoid safety and financial impacts.

The LyondellBasell Journey

The LyondellBasell journey to a more secure OT environment is not unique in the operating industry. Over time, the company's focus has changed from a collection of security initiatives to a cohesive risk management approach. Our journey started in 2011 with the addition of a new Chief Information Security Officer (CISO) and his wealth of cybersecurity experience. Under new

leadership and with the full support of the executive committee, the company shifted from a reactive security program to a proactive risk management program. At the time, the plants had a near impenetrable line of demarcation between IT and OT systems.

One of the first significant efforts was the development of the LyondellBasell IT Policies and Standards. These documents were created from scratch and supplemented using existing Sarbanes Oxley (SOx) controls. Previous attempts were disorganized and unsuccessful, oftendue to a lack of alignment on vocabulary. The successful adoption of policies and standards provided the bedrock for LyondellBasell achieving the internationally recognized risk management ISO 27001 certification in 2012.

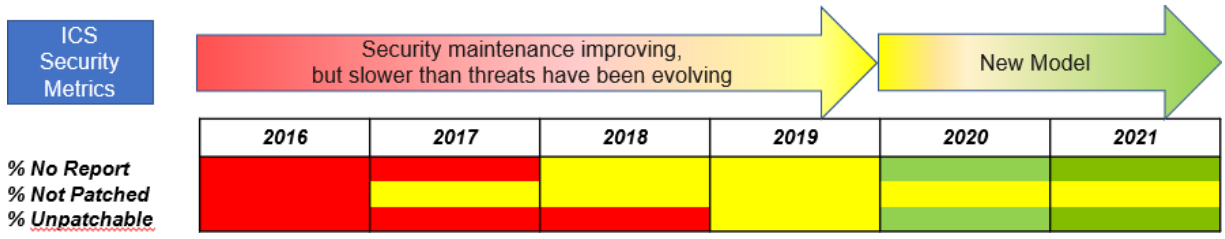
The company knew that a virus infection on the OT systems was a strong possibility. If this ever occurred, due to the implementation of the Purdue Model, the infection most would be contained. Due to the proximity to the Corporate Zone (Level 4) and the high usage of USB ports for managing that layer, the infection would have a high probability of occurring on our monitoring layer (Level 3 of the Purdue Model). If this occurred, the result could be a plant shutdown and an impact on the plant monitoring systems and advanced control. Operations would be impacted for an extended periodof time. We recognized that we were vulnerable in a few key areas; the misuse of jump drives on the OT network, patches not being current, and out of date virus protection.

Our leadership realized these vulnerabilities transcended throughout all sites globally. LyondellBasell plants operated with considerable autonomy and little standardization regarding patching and virus updates. Our corporate standard addressed USB hygiene, but not all sites were adequately following the standard on the OT network. At that time, no corporate standard was directly applied to the OT network. Essentially, we realized this type of event could occur in any of our plants. As a result, executive management pushed for the centralization of the cybersecurity program.

The first step in this process was standardizing the architecture of the OT network through a centralized program. A global survey was conducted at all LyondellBasell plants to identify the OT network gaps. The survey identified several plants without functioning firewalls separating the IT and OT networks, insecure remote access, patching not being done, and little to no monitoring of the systems on the OT network. As a result, a yearly program was initiated that invested in OT network segmentation, centralized server updates for patching and antivirus, secure remote access and security monitoring. The program was funded entirely through the central IT budget, removing the barrier of competing for plant budgets.

Once the architecture was standardized on our OT networks, IT began tracking our progress utilizing Key Performance Indicators (KPIs). The three key KPIs selected to drive improvements and lower the risk were Percent Devices Not Reporting, Percent Devices Not Patched and Percent Obsolete Devices Not Isolated. When we first began measuring these KPIs, the company's performance was unacceptable (as shown below.) Reports and frequent updates were shared with the executive leadership, which increased the focus and acceptance of the program. As a result,

year-to-year improvement occurred, resulting in our current situation where all three KPIs are in an acceptable range. More improvement is needed, but significant progress has been made.

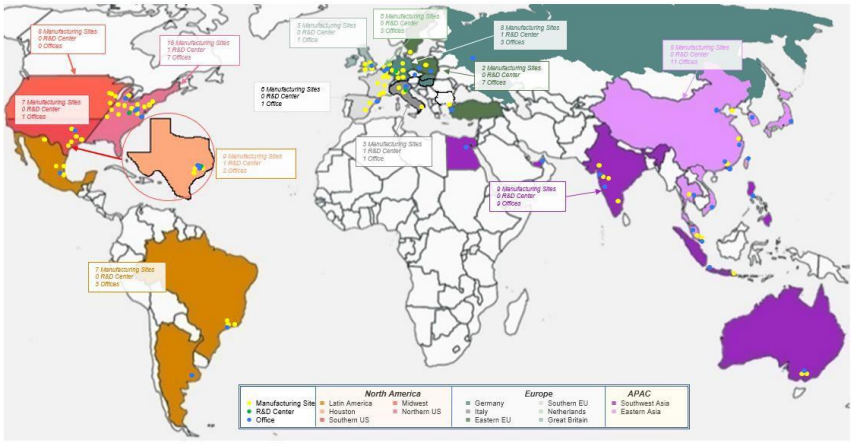


The next step in the process was the development of a standard that applies to the OT networkin the area of cybersecurity. A new standard was developed utilizing the existing management processes in manufacturing (i.e., our operational excellence (OE) structure). The OE process requires regular auditing at the plant level with tracking of identified risks at the executive levels of the organization. Depending on the level of severity, the manufacturing executives monitor progress and ensure closure of these risks.

One essential facet added as part of the transformation is third-party assessments of our cybersecurity program. These assessments are done on a three-year cycle and are focused onthe overall health of the cybersecurity program and how we compare against our peers. The assessment results are used to generate findings and reported to the highest levels of the company. The findings help drive changes and improvements in the programs and help focus on areas for the future.

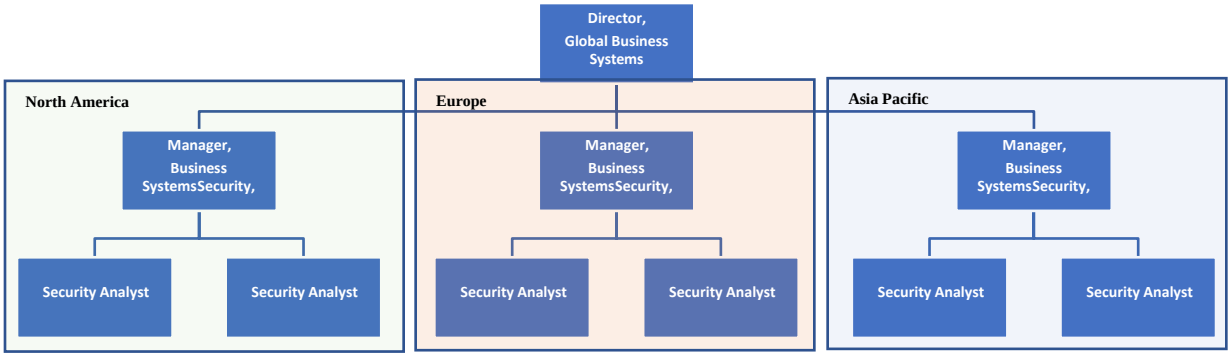
Developing OT Talent Pipeline

We decided to create a center-led organization with regional coverage focused on OT cybersecurity. Each plant had someone from the group assigned physically or near provide regional coverage. With over 90 plants in the LyondellBasell system, having someone located at every plant posed a challenge – thus the need to create regional clusters to meet that need.



The new organization, Business Systems Security, reports to the Senior Director of Digital Security and is a peer organization to the CISO. The Digital Security organization became a

standalone workstream, aligned side-by-side to the IT function, reporting to the same Senior Vice President as the CIO, making the Digital Security separate and autonomous from IT.



The Business Systems Security organization was built completely from scratch. The security analyst's job function is to act as an ambassador for cybersecurity in the plants, ensuring the plant systems and networks comply with corporate standards and communicate threats appropriately. The position serves as the Level 2 support during incident response, monitoring and site vulnerability assessments. The team ensures the security awareness program is effective and assists with technical direction and strategy for OT systems architecture and security.

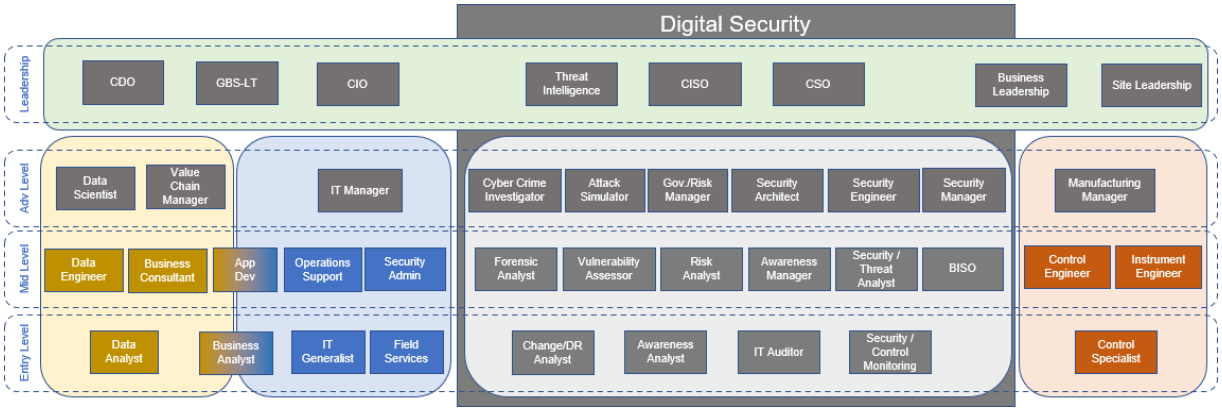
The requirements of the positions cross both the IT and OT spectrums. Working knowledge of technologies such as Microsoft Windows, Active Directory and domain architecture and management, along with plant systems such as Modbus, OPC, and DCS systems, are neededto be successful. Experience is necessary in the area of developing and refining risk-based, defense-in-depth security architectures using established frameworks such as the National Institute of Standards and Technology (NIST) or International Organization of Standardization(ISO). Also, experience with security incidents and event analytics and certifications such as Certified Information Systems Security Professional (CISSP) are needed.

The strategic approach to filling the organization focused on staffing experts with backgroundsin either IT or OT systems. Roughly half of the new candidates in the organization came from LyondellBasell plants where they filled roles as systems administrators on the OT side. The other half were formerly IT professionals. Candidates were hired both from within the companyas well as outside the company.

To mitigate any gaps in knowledge of the security analysts in either the area of OT systems or cybersecurity, a formal training program has been developed focused on the nuances of the position. Everyone in the organization, including management, are encouraged to complete the training. For the future, an internal certification is being developed which will be required for all security professionals. Manufacturing cybersecurity will be included in the certification. CISSP certification is also highly recommended.

As the organization continues to mature, one of the biggest challenges will be finding and retaining talent. Partnering with local universities and building a strong intern program has assisted with identifying talent for the future. To assist with retention, a clear technical ladder has

been developed, allowing for the organizational movement into other roles within cybersecurity, IT, or manufacturing. This training is an investment into careers with the intent tobuild committed, knowledgeable employees.



Closing

Building a robust digital security program takes time and focus. The focus includes a risk management process, including OT, and developing a talented resource pool for addressing the continuing challenges. The changing threat landscape requires a constantly evolving program to stay ahead. LyondellBasell, like you, is on this never-ending journey.