WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Intellectual Property Theft in Operational Technology Environments

Examining Cyber Risk to Manufacturing Processes

JOSH HANRAHAN | SENIOR ADVERSARY HUNTER
SETH LACY | PRINCIPAL ADVERSARY HUNTER
APRIL 2023

TABLE OF CONTENTS

Growing Threat of IP Theft in Industrial Environments

Intellectual property (IP) theft as a component of broader adversary information operations is an enduring and acknowledged risk, but one which is more often referenced in relation to enterprise IT environments than operational technology (OT) networks. This does not mean that OT networks are somehow immune from this threat – in fact, given that in many cases IP information is hardcoded into the processes OT networks manage, they should be prioritized for protection from the risk of IP theft.

IT and OT networks are increasingly interconnected, and efforts to support digital transformations continue to blur the boundaries between these previously distinct network domains. The imperatives for remote work and remote access imposed by the COVID-19 pandemic only served to accelerate this new paradigm of interconnectivity.

Increasing interconnectivity between IT and OT networks creates opportunities and incentives for adversaries to pursue their IP theft objectives within OT network environments, particularly if the adversary cannot meet their objectives through enterprise IT network compromise alone. For network defenders, it is important to consider the risk of IP theft in OT environments within the wider context of industrial espionage. Historical adversary efforts at IP theft from enterprise IT environments are well documented and have been examined and relayed as a serious risk to industry for over a decade.[1]

The U.S. consulting firm Deloitte has studied and attempted to quantify the risks to a business of IP theft through cyber espionage, concluding that "IP theft has ramifications that are harder to grasp: fewer up-front, direct costs but potential impacts that might metastasize over months and years. Theft of Personally Identifiable Information (PII) might quickly cost customers, credit ratings, and brand reputation; losing IP could mean forfeiture of first-to-market advantage, loss of profitability, or—in the worst case—losing entire lines of business to competitors or counterfeiters."[2]

Given the potentially high returns on time and effort invested for those adversaries focused on IP theft, it's not surprising that the security community has observed multiple groups targeting networks in pursuit of protected IP for over a decade. While many of these incidents have historically been detected in enterprise IT environments, this disproportion is also influenced by disparities in visibility and monitoring between the two network types. The scope of the incidents is indicative of the extent of the potential threat and OT networks themselves have not been excluded from adversary targeting and operations.

Adversaries attributed by a broad range of other organizations to Chinese state sponsorship are regularly cited as particularly aggressive in their efforts at cyber-related IP theft. This included a 2014 U.S. Department of Justice grand jury indictment of five hackers affiliated with the People's Liberation Army (PLA), as well as a 2018 report from the United Kingdom's National Cyber Security Centre (NCSC) which detailed broad targeting of the networks of UK organizations for IP theft.[3,4] The U.S. Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure

1 **The Cybersecurity Threat to U.S. Growth and Prosperity** – McKinsey

2 **The hidden costs of an IP breach** – Deloitte

3 **U.S. Charges Five Chinese Military Hackers for Cyber Espionage** – Department of Justice

4 **Alert: APT10 Continues to Target UK Organisations Across Wide Range of Sectors** – NCSC

Security Agency (CISA) issued a joint advisory in May 2020 that discussed Chinese-affiliated cyber operators targeting of COVID 19-related research and IP.[5] Additionally, in a July 2022 joint statement by FBI Director Christopher Wray and United Kingdom Security Service (MI5) Director Ken McCallum, both continued to warn of the risks of IP theft and industrial espionage emanating from China.[6]

Similarly, the United Kingdom's National Cyber Security Centre (NCSC) and Canada's Communications Security Establishment (CSE) released a joint Advisory in July 2020, detailing the activities of Russian state-sponsored cyber actors targeting COVID 19 vaccine development in their respective countries. The authors of the advisory assessed it was highly likely that the adversaries intended to steal information and IP related to vaccine development and testing.[7]

Dragos assesses with moderate confidence that adversaries are most likely to pursue IP theft in OT environments as part of a broad campaign and that the sensitive information an adversary can acquire from an OT network may not be available in other parts of a company's network. Within enterprise IT network segments, sensitive IP is increasingly stored offline or within closely guarded network enclaves. In contrast, on the OT side of the network, this IP is likely to be embedded into the processes the OT network manages and may be impossible to separate from the OT network's operation. This information includes details on the amounts of inputs or ingredients, and the specifics of the processes applied that transform these raw materials into a finished product or substance.

This potential disparity in information availability and protection could drive an adversary to pursue information from an OT network that they cannot access in other parts of a company's networks, particularly in cases where the protected IP is inherent to an OT network's management of critical production processes.

Manufacturing Process Influence on Information Availability

The type and value of information that can be extracted from an OT network by a motivated adversary will depend in part on what type of manufacturing process the targeted network manages. Manufacturing processes can be broadly divided into three categories – batch, continuous, and discrete.

These three categories can be further divided into two groups, the first encompassing batch and continuous manufacturing processes and the second consisting of discrete manufacturing processes.

The main difference for the purposes of IP theft is that discrete manufacturing processes produce a single product from a defined bill of materials, while batch and continuous manufacturing processes rely on a "recipe," or formula, to define how to combine amounts of raw materials to yield an expected quantity and quality of the finished product. The inputs to discrete manufacturing processes are generally fixed and predictable, while multiple variables can impact batch and continuous manufacturing processes, requiring adjustments to both the inputs and the process itself.

5 **People's Republic of China (PRC) Targeting of COVID-19 Research Organizations** – FBI and CISA

6 **Joint U.S.–UK Statement on Risk of Chinese Corporate Espionage** – Federal Bureau of Investigation

7 **Advisory: APT29 Targets COVID-19 Vaccine Development** – NCSC and CSE

These differences influence the type of information an adversary would hope to obtain when targeting IP in an OT network environment, as well as additional data an adversary might pursue from other networks and sources. This also influences how damaging the loss of proprietary information from an OT network could be, depending on the sensitivity of the information in question.

Batch Manufacturing

Batch manufacturing processes are likely to be lucrative for an adversary from the perspective of IP theft. The step-by-step nature of batch processing, and the fact that each step must be completed in its entirety before moving to the next step in the process, could provide an adversary an opportunity to extract the amounts of each input into the process and the set points from the controllers for the equipment involved in the process.

This would require the adversary to observe the batch process from start to finish as the raw materials and ultimately product moved through each of the distinct steps. The total time to completion for a batch process may influence the amount of time an adversary would need to be in the OT network and observing the process to be able to potentially reverse engineer the totality of the process.

A data historian overseeing and recording data on a network's operation can be a logical initial target for an adversary attempting to gather IP information out of an OT network overseeing a batch manufacturing process, as these devices aggregate and store data over a longer time horizon. That said, in some cases the information held by the historian may be raw sensor data lacking the necessary context. This lack of context can sometimes be a purposeful design decision in networks overseeing processes derived from sensitive IP. In these cases, human machine interfaces (HMIs) or supervisory control and data acquisition (SCADA) devices can also be important targets, as their data is meant for operator consumption and therefore unit-scaled with full context.

These devices could provide an adversary with valuable data and context to use in efforts to reverse engineer the recipe for the product being produced. These recipes are the most sensitive category of IP for many companies in the pharmaceutical, chemical, and food and beverage industries. In some instances, this category of IP can represent billions of dollars in research and development for new pharmaceuticals and chemicals, and its loss or theft by an adversary could have significant repercussions for the competitiveness and profitability of the company targeted by an adversary.

Continuous Manufacturing

Continuous manufacturing processes share many similarities with batch manufacturing in that predetermined amounts of raw ingredients are combined and modified by equipment to produce expected quantities of a finished product. The major difference between the two approaches is that in contrast to the necessity to complete each step in a batch process prior to moving to the next step in the process, the materials in continuous manufacturing move seamlessly through the steps of the process without pause. The product is tested throughout the process for adherence to expected (and in many cases mandated) quality levels.

Given that the materials in a continuous manufacturing process are moving seamlessly through all the steps of the process at any point in time, the set point values for the controllers managing the process are also always active. A properly functioning continuous process should not vary over time, and a varying continuous process is considered to be statistically "out of control" and in need of correction.

Therefore, if an adversary can capture a snapshot of the set point values for a continuous process even over a relatively short time horizon (measured in minutes, not hours), if that data is sufficiently rich in context, the adversary may have all the information they need to reverse engineer the process in question. This is mainly because the set point values for the process should remain relatively static once the continuous process is initiated.

While data historians remain a logical initial target for an adversary targeting IP contained within a continuous manufacturing environment, the same caveats from batch manufacturing environments surrounding the level of context contained within the historian's data still apply. If this data lacks context based on purposeful or incidental design, an adversary may need to seek additional context from unit-scaled data in an HMI, SCADA, or similar operator-focused device. If the necessary context is not available or is purposefully obfuscated in those devices, the adversary may be forced to pursue additional information from other data sources or networks to effectively reverse engineer the process in question.

Discrete Manufacturing

Given the fixed inputs that characterize discrete manufacturing, there is generally less information of relevance from an IP theft perspective for an adversary to extract from an OT network overseeing a discrete manufacturing process. That said, there is some information of interest or value for adversaries contained within these networks.

In the case of discrete manufacturing, rather than being interested in the components and inputs that result in a finished product (much of which could be determined through examination of a bill of materials or disassembly and reverse engineering), an adversary would instead be seeking information on the manufacturing process itself. Information on manufacturing processes can be significant, as efficiencies in these processes can allow a company to produce a certain product more quickly and at a lower cost, which in turn enables the company to offer the product to consumers at a lower price while maintaining an acceptable profit margin.

These types of processing efficiencies can be vital in maintaining a company's competitive edge, particularly in industries and products where the main differentiating factor from competitors' offerings is price. In these instances, information gleaned from an OT network on the layout, functionality, and configuration of the network's components could be of value from the perspective of an adversary, especially if combined with additional information on engineering and design from other networks and sources – for example, network and engineering diagrams from an OT systems integrator.

Implications Beyond Information Loss

While adversaries may target an OT network with the goal of extracting specific information relevant to a company's closely held IP, the loss of this information may not be the extent of their impact on a company's operations. The general fragility of OT networks and the necessity of uninterrupted availability in most instances mean that even skilled adversaries run the risk of having a negative impact on the operations of an OT network they do not fully understand, particularly from a process perspective.

This risk could be amplified in instances where an adversary whose primary responsibility is targeting IP on enterprise IT networks pursues IP within an OT environment. An adversary "learning" about ICS and industrial processes within an OT network is at high risk of causing unintentional disruptions and network failures. As an example, an adversary actively scanning with a tool like Nmap, which adversaries commonly deploy in the discovery phase of MITRE's enterprise ATT&CK matrix, is at high risk of placing industrial devices into a denial-of-service state and taking down an OT network when the adversary runs the same tool in an industrial environment.

Even in the case of skilled adversaries, who understand the functionality of OT networks and the constraints necessary to interact with the networks with minimal risk of disruption, there can be tension between the pursuit of IP and the preservation of network availability. This can be further influenced by the level of the network where adversaries are seeking information.

The manipulation or exploitation, deliberate or unintentional, of HMIs, SCADAs, or historians at Levels 2 or 3 could eventually cause malfunction or disruption of physical processes and machinery at Levels 0 and 1. Furthermore, an adversary attempting to extract settings and configurations directly from Level 1 devices, such as programmable logic controllers (PLCs), safety instrumented systems (SIS), or remote terminal units (RTUs), is at even higher risk of causing network disruptions or malfunctions, given the closer proximity and criticality of these devices to the physical processes being controlled by the OT network.

German Steel Mill Case Study

In December of 2014, the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI), in English known as the Federal Office for Information Security, detailed and released a report on its findings for the year.[8] This report provided insight into a 2014 event when a malicious actor infiltrated a German steel facility. The adversary's final impact caused multiple controls to fail and critical process components to become unregulated, which ultimately caused significant physical damage to the steel mill.

The intrusion began with a targeted spear-phishing email which, when executed, enabled the adversary to gain an initial foothold on the IT network of the victim. Dragos assesses with moderate confidence that due to the highly targeted nature of the spear-phishing email, sophisticated social engineering tactics that the adversary used, and the adversary's follow-on actions, this activity set was a targeted operation against the victim.

Once the adversary established initial access, they then compromised the victim's domain controller and accessed the user credentials of the victim's OT network. After obtaining these credentials, the adversary pivoted into the OT network by enumerating OT assets and employing lateral movement techniques. While the victim's network was not completely flat, maintaining some separation between IT and OT, it had areas where traffic could transverse the two zones freely and allowed the adversary to access the OT network easily once the credentials were stolen.

8 **Die Lage der IT-Sicherheit in Deutschland 2014** – BSI

Once access to the plant network was achieved, BSI explained that the adversary's observed activities were "very advanced." Additionally, BSI stated, "The compromise extended to a large number of different internal systems, including industrial components. The attackers' know-how was not only very pronounced in classic IT security but also extended to detailed specialist knowledge of the industrial control systems and production processes used."[9]

German steel is well regarded globally for its high tensile strength and durability and is considered "boutique" in nature. German steel ventures invest many resources and money into research and development of new ways to construct steel. These characteristics, along with cutting-edge technological advancements in steel manufacturing technologies, make German steel organizations a prime target for state-sponsored efforts toward IP theft.

Steel manufacturing is a complicated continuous manufacturing process that involves multiple industrial components and procedures. Typically, IP in steel Manufacturing is less contained in documents that can be stolen and found more in the specific measurements and signals sent to industrial control sensors in a certain way. Elements such as timing intervals when certain actions occur or the quantities of materials and in what order they are added help shape the recipe for the steel manufacturing process.

This recipe is essentially the IP that is valuable to adversaries. Information about how industrial control processes interact with ICS devices in the Process or Level 0 layer of the Purdue model is logged in a centralized database called a data historian. Therefore, as noted above, if an adversary intends to steal intellectual property related to steel manufacturing, the data historian is a logical first target.

When the adversary was operating within the German facility's OT network, they made mistakes that led to cascading failures within the operations environment, which ultimately damaged the blast furnace. The failures caused by the adversary occurred over the course of weeks. Most likely, the steel mill engineers were addressing the failures as an operations event and not a malicious intrusion event. BSI's report stated, "Failures of individual control components or entire systems increased. The failures meant that a blast furnace could not be shut down properly and was in an undefined state." This activity stopped the blast furnace from being shut down safely, resulting in massive physical damage to the furnace.

While we cannot fully understand the intent of the adversary (the only entity that can truly understand the intent of the attack is the actual adversary), Dragos assesses with low confidence that the adversary's primary tasking was IP theft and not physical destruction or cessation of critical operations, and that the adversary was attempting to extract information from the victim's data historians.

The destruction of the blast furnace resulted in an evacuation of the steel mill. Fortunately, no one onsite was seriously injured; however, the operational and financial fallout from this event could have lasted for years. Every day the furnace is not operational is a loss for the company and the employees working at the site.

Deconstructing, planning, designing, and rebuilding a blast furnace is neither a quick nor inexpensive exercise. In 2007, a blast furnace in Dearborn, Michigan, was dismantled to make way for a new furnace.[10]

9 **A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever** – Wired

10 **L-169 members tear down, rebuild blast furnace in under 100 days** – Boilermakers.org

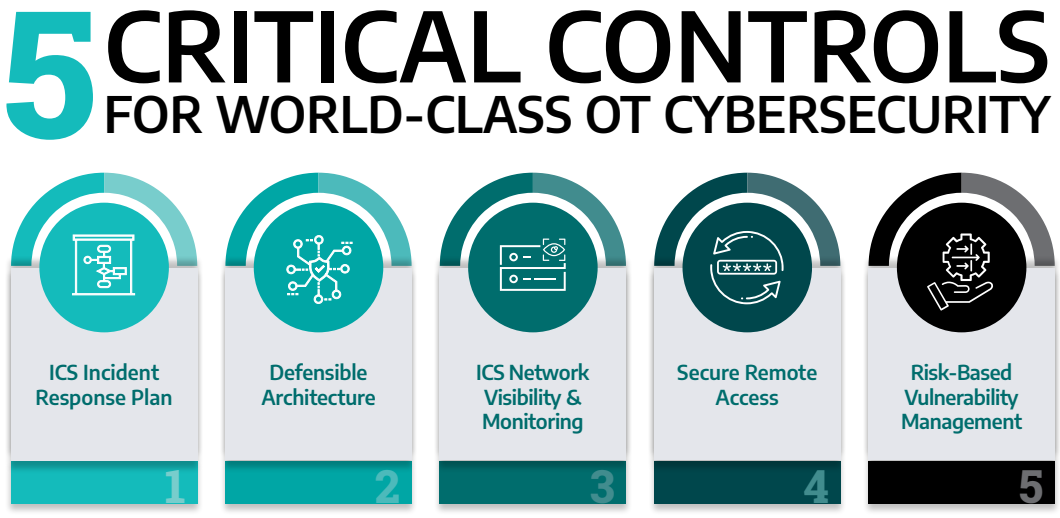
In a record-breaking attempt, over 250 boilermakers and 1000+ staff onsite performed the planned demolition and rebuild of the blast furnace in 97 days. However, this involved staff working 12-hour days for 97 days straight. Additionally, the pull-down and rebuild were a part of a USD 750 million revitalization project planned years in advance. So, in the case of the German steel mill, if everything was pre-planned, with the staff working 97 days straight without a break, and if there were no setbacks due to supply chain issues or other problems, the facility would still be losing money and could not produce a product for well over three months. The financial impact of this alone would be devastating. More realistically, factoring in supply chain issues and wait times for critical pieces of the new furnace, the rebuild process would likely have taken years if the company even chose to pursue the rebuild.

Five Critical Controls For OT Cyber Defense

To protect against these risks and related threats, Dragos recommends the **5 Critical Controls for World-Class OT Cyber Security** [11] identified by the SANS institute - which presents a framework for implementing a world-class OT cybersecurity program to defend against adversary activity directed against OT networks, be it IP theft, ransomware, or targeted cyber-physical effects.

A first step in implementing these controls is achieving executive alignment on the role and importance of OT cybersecurity and the specific risks an OT cybersecurity program is meant to defend against. In this case, the risk of IP loss or OT network disruption as a result of adversary efforts to steal sensitive IP from an OT network.

One potential way to achieve this organizational alignment is to tie the effort back to real-world scenarios and previous incidents. As in the case study above, research previous attacks and understand their relevance to your business. Extrapolate previous incidents into relevant scenarios that incorporate the unique aspects of your environment and capture how a similar loss of valuable IP or disruption would impact your company and its operations.



11 The Five ICS Cybersecurity Critical Controls – SANS

Conclusion

IT and OT networks are increasingly interconnected, a dynamic driven by diverse forces spanning from unprecedented global pandemics to support for broader digital transformations. This increasing interconnectivity continues to blur the boundaries between these two previously distinct network domains and has been accompanied by a spillover of threats more generally associated with IT into the OT network space.

IP theft through cyber means is no different, and increasingly robust protections for sensitive information in the enterprise IT realm can create a disparity in information availability and protection that could drive an adversary to pursue sensitive information from a company's OT network, which they are unable to access elsewhere.

Given that for many OT networks, valuable IP is hardcoded into the processes and operations the networks oversee, options for mitigating risk are somewhat circumscribed by this central reality. Accordingly, these network segments should be prioritized for incident response (IR) planning, increased visibility, and robust monitoring.

Dragos assesses with moderate confidence that adversaries will pursue IP theft in OT environments as part of broad campaigns and that network devices which aggregate and store data over longer periods, such as data historians, will remain a logical first target for adversaries targeting IP within OT network environments. This is especially true for networks overseeing continuous and batch manufacturing processes.

Dragos has observed a steady growth in both threat activity and the diversity of industrially focused adversaries since 2017.[12] While defending OT networks and the valuable intellectual property resident within them from adversary threats is potentially challenging, there are tools, community resources, and partners positioned to assist companies along this journey.

12 **Year in Review 2022** – Dragos

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.