PREVENTING INTELLECTUAL PROPERTY THEFT IN ADDITIVE MANUFACTURING

by

Matthew L. Scott

A Directed Research Project

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

School of Engineering Technology

West Lafayette, Indiana

May 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Duane Dunlap, Chair
Purdue University
Mr. Terrence McGowan, Associate Technical Fellow, Chief Architect
Aerospace Company
Mr. Hemanth Kumar, Manager
Aerospace Company

Approved by:

Dr. Duane Dunlap
Head of the Graduate Program

The research and evaluations in this capstone project are dedicated to the technologists and engineers in pursuit of the optimal methods for additive manufacturing data and intellectual property protection

ACKNOWLEDGMENTS

Working alongside brilliant people through the pursuit of the Engineering Technology master's degree has been my honor. Terry McGowan has provided inspiration and guidance on key technological concerns in the additive manufacturing industry. I would also like to extend my gratitude to Ousmane Loum for his expertise in information security and cryptographic knowledge.

Without a firm grasp on today's technologies, a proposal for improvement can't be made. Jose Jacinto has been a tremendous help to keep me driving forward when I've felt stuck finding solutions. Admiration goes to Dr. Hutcheson for his disciplined agile approaches to solving big systemic challenges. Professor Hedrick has gone above and beyond to provide guidance on the difficult concepts in information security. Lastly, my deepest appreciation goes to my wife, Diane, for being the constant and encouraging force I've needed to accomplish more than I could do alone.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AM – Additive Manufacturing

R&D – Research and Design

OEE – Original Equipment Effectiveness

CIAN – Confidentiality, Integrity, Availability, Non-Repudiation

IP – Intellectual Property

PBF – Powder Bed Fusion

DMLS – Direct Metal Laser Sintering

CAD – Computer Aided Design

FEA – Finite Element Analysis

DE – Design Engineer

SE – Stress Engineer

PLM – Product Lifecycle Management

STL – Standard Tessellation Language

NC – Numeric Code

TXID – Transaction Identifier

PoW – Proof of Work

PoMW – Proof of Manufacturing Work

REST – REpresentational State Transfer

SOAP – Simple Object Access Protocol

HTTP – HyperText Transfer Protocol

FEPC – Front-End Personal Computer

LAN – Local Area Network

PtP – Point to Point

OT – Optical Tomography

MP – Melt Pool

API – Application Programming Interface

3D – three dimensional

2D – two dimensional

TB – Tera-Byte

IT – Information Technology

SM – Supplier Management

ENG - Engineering

InfoSec – Information Security

QE – Quality Engineering

QA – Quality Assurance

RBS – Risk Breakdown Structure

GDP – Gross Domestic Product

GLOSSARY

Additive Manufacturing – "process of joining materials to make parts from 3D model data, usually layer upon layer, as opposed to subtractive manufacturing and formative manufacturing methodologies" (ASTM, 2015).

Powder Bed Fusion – "additive manufacturing process in which thermal energy selectively fuses regions of a powder bed" (ASTM, 2015).

Build file – a monolithic file containing all machine instructions for additive fabrication

Insitu Inspection – "NDE measurements [can be] conducted during the manufacturing process and process measurement data on-the-fly" (Hirsch, et al., 2017)

Digital Thread – "a single, seamless strand of data that stretches all the way from the initial design concept to the finished part, constituting the information which enables the design, modeling, production, validation, use, and monitoring of a manufactured part" (Trouton, Vitale, & Killmeyer, 2016).

Attack Vector – "a segment of the entire pathway that an attack uses to access a vulnerability. Each attack vector can be thought of as comprising a source of malicious content, a potentially vulnerable processor of that malicious content, and the nature of the malicious content itself" (Guild to Data-Centric Threat Modeling, p. 5).

Gross Domestic Product – "The value of the goods and services produced in the United States" (Bureau of Economic Analysis, Gross Domestic Product, 2018). The calculation is Personal Consumption Expenditures + Investment + Government Spending + Net eXports. The equation is then (C+I+G+(X-M) =GDP) (Bureau of Economic Analysis, Gross Domestic Product, 2018)

ABSTRACT

Author: Scott, Matthew, L. MS
Institution: Purdue University
Degree Received: May 2019
Title: Preventing Intellectual Property Escape in Additive Manufacturing
Committee Chair: Duane Dunlap

Advanced manufacturing machines, especially for additive manufacturing, are taking advantage of the latest technologies for maximum optimization and precision. Efforts to communicate the complex information, however, can leave systems vulnerable to various attacks both from inside and outside a company's network. Intellectual property theft attack vectors must be fully understood and accounted for within the information security framework. Software solutions, such as blockchain, will enable full transactional accountability needed to ensure theft cannot occur throughout the manufacturing lifecycle. The resultant research and expert interviews provide a thorough analysis of the elements at risk for which blockchain opportunities will mitigate.

CHAPTER 1. INTRODUCTION

1.1 Problem Statement

A single additive manufacturing (AM) build instruction file holds the complete instructions on how to manufacture an object as good as the original. The need to protect files from cybersecurity threats is paramount to the success of engineering companies (Chen, Mac, & Gupta, 2017, p. 183). If complete build instruction files are not managed with secure information technology methodologies, intellectual property escapes will result in negative outcomes. Substandard parts, company lost profits, and compromised safety are a few of the possible consequences (Straub, 2017, p. 2.4). Intellectual property security must be established on a part or build-by-build basis with cybersecurity compliance measures accounting for all possible attack taxonomies (Yampolskiy, et al., 2018). "Secure Cyberspace" is the related engineering challenge with the need to protect digital manufacturing instruction files, networks, and machines throughout a product's lifecycle (Secure Cyberspace, 2018).

1.2 Scope

The AM process, current and future cybersecurity best practices, and blockchain opportunities were the scope of this project. Additive manufacturing is the layer-by-layer fabrication process in which different types of materials are fused together with various advanced technologies. The metal powder bed fusion (PBF) technology, specifically direct metal laser sintering (DMLS), and related data were the technology focus. Due to the current industry need for rapid structural component fabrication, metal 3D printing is a competitive market. The related digital thread was reviewed to account for the need of advanced simulations. The “digital twin”, or data representing a manufactured component at any point in the process, brings first time quality.

Manufacturing businesses must continually balance cost, schedule, and quality. However, a fourth factor distrupts the trifecta very easily – cybersecurity. An unknown number of impacted companies decide to reshore manufacturing to minimize the security risks. Hartman, Ogden, & Hazen (2016) state:

> As security breaches and piracy problems continue to proliferate, the need to retain and protect intellectual property and other proprietary information will increasingly influence firms to reshore functions to geographically closer, trusted partners. Yet, problems controlling proprietary information typically will not necessarily result in insourcing. (p. 215)

Insourcing is possibly not the optimal cost-effective decision. Product-originating companies, however, must understand and protect the AM digital thread before sourcing the advanced manufacturing work to a partner company.

Certification of a 3D-printed metal part is incredibly difficult due to "more than 130 parameters that govern the metal additive manufacturing process" (Yampolskiy, et al., 2018, p. 440). Organic geometric complexity is available to engineering designers now through advanced computer-aided design (CAD) software. The costs involved in research and development (R&D) moving to production scale are burdensome and difficult to realize cost savings. An estimate was run for a 3cm length x 3cm width x 10cm height part. Other costs were a two-inch titanium build plate, titanium powder, all labor, and post-processing, which came to $5,655 average cost per part. See Table 1.1 for detail-level cost breakdown from the MITxPro *Additive Manufacturing for Innovative Design and Production* course calculator (Hart, 2018).

Table 1.1 Total cost for sample production AM part

	%	$
Material	20.4%	$5,759
Build prep	2.5%	$700
Machine usage	39.0%	$11,020
Build consumables	29.4%	$8,302
Labor	8.2%	$2,317
Post-process	0.6%	$174
Total cost		**$28,273**
Average cost per part		**$5,654.65**

Once the process and costs are understood and reduced due to optimization, suppliers can then be utilized for mass production capabilities. However, at this point the digital thread needs to leave the corporate, internal-protected intranet to communicate with the supplier or partner. Optimization is key to success, so a robust and secure solution for communications is mandatory.

Figure 1.1 depicts the scope of the mentioned R&D fabrication process and eventual supplier connection for production scale. Multiple types of files are now generated in and around additive manufacturing. A full but not exhaustive set of metal AM data is contained in the pink region. From top to bottom: the build file, insitu-inspection, optical tomography, melt pool, and machine original equipment effectiveness (OEE) data are shown. A supplier would then take over the fabrication process with a proven build file and continue the post-processing, inspection, and delivery processes. Deeper review of the data types and their significance will be addressed later in the writing.

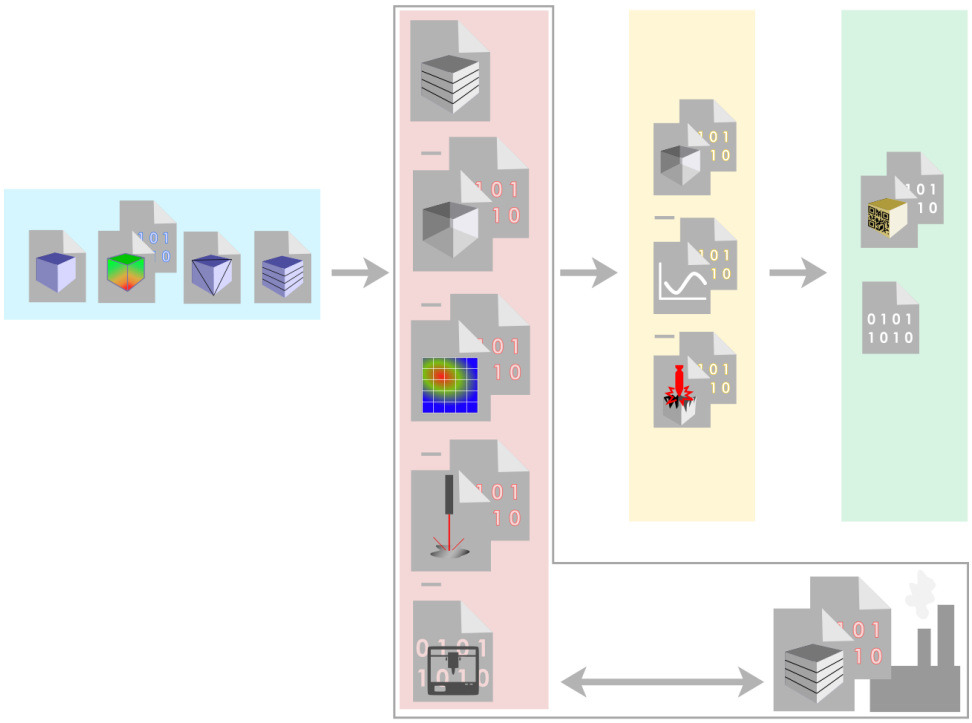


Figure 1.1 High-level depiction of all types of AM data and highlighted scope

Cybersecurity is becoming increasingly difficult to manage as more devices are connected to centralized networks to track and utilize the digital thread (Dibrov, 2017). Optimization is mandatory to compete in the aggressive aerospace industry, for instance. The resultant paradigm is now shifting to the blockchain technology because of its inherent alignment to confidentiality, integrity, availability, and non-repudiation (CIAN). Non-repudiation, or adherence to agreements, is an additional cybersecurity best practice to ensure plan consistency between two or more parties.

Gale (2017) states, “According to Cybersecurity Ventures, the annual cost of cyberattacks is expected to increase from $3 trillion in 2015 to $6 trillion by 2021” (p. 14). The exponential growth in costs due to cyberattacks necessitates a full understanding of the technologies available to protect and propel business. Corporations, with 500 or more employees, typically employ robust information security technologies. However, a company’s ability to fully implement a connected factory is dampened by the fear of cyberattacks. Dibrov (2017) says, “When it comes to connected devices, the massive numbers that will be in use in businesses make it impossible for people on their own, or for understaffed IT and security teams, to manually identify and stop risky activity” (p. 4). The case, then, is to reduce risk by employing an intelligent system.

Additive manufacturing devices can run while disconnected from a network. However, the IoT capabilities and other sensor data, from the mentioned new devices, compel a business to optimize with that data. Focus was then be placed on AM due to the forward-reaching possibilities of a fully automated factory. To obtain the data in a real or near-real time way, the device must be connected to the network.

Protecting intellectual property (IP) in AM is the goal of this project. The proposal was to gain understanding of the cybersecurity threat taxonomies, identify known gaps, and propose a technology solution. The target technology, then, is blockchain, which will be adapted to the additive manufacturing digital thread needs.

Chapter two will contain the review of literature to support the proposal. Primarily, a complete analysis of the AM process facilitated potential security gaps comprehension. Alignment of security best practices using the CIAN methodology served as a framework from which to build. Demystifying the blockchain technology revealed how it is best suited for the IP security proposal. Also, understanding storage technologies and techniques served the digital thread needs for file correlation. Finally, a grasp on cybersecurity attack taxonomies, specific to AM, facilitated the tabulation of the process for filling the security gaps.

Chapter three brings all the information together to define a new best practice for filling the security gaps. The attack taxonomies were laid out with the proposed technology solutions. Lastly, a matrix containing key persons, security risks, and key attributes of the technology which fills the risk gaps were defined. The results served as a standard with which to apply internal business regulations for security conformance.

1.3 Measure Limitations

The measurement method came with limitations. Cybersecurity attacks have occurred, and proof has been given from the impacts. However, there is not a current way to measure impact prevention based on security methods chosen. Instead, this project focused on interview responses for probability ranking (1-low to 5-high) verses negative impact ranking (1-low to 5-high). One expert from AM technology, one from blockchain technology, one from infrastructure technology, and one from blockchain architecture, will ranked the risks. Overall percentage and high-priority score from the four experts were calculated for the final scoring.

Haimes (2015) stated that "risk and uncertainty arise from measurement errors and from the underlying variability of complex, natural, social, and economic situations" (p. 44). The complex and natural factors involved in cyber security risk assessment, tied to expert opinions, can lead to measurement errors. The expert rankings were guided in such a way that unbiased and informed opinions were made. Clearly defining probability and exact negative impacts was necessary.

CHAPTER 2. REVIEW OF LITERATURE

2.1 Additive Manufacturing and the Digital Thread

A thorough analysis of the additive manufacturing process was necessary to identify every point data is accessible and informative (Figure 2.1). The process initiates when a computer aided design (CAD) digital file is created by an engineer. The integrated finite element analysis (FEA) solver aids the design engineer (DE). The stress engineer (SE) is also aided but by providing simulated stresses on the designed part. The resultant analysis file is now carried with the part design file to a product lifecycle management (PLM) repository. The CAD file is used to generate a standard tessellation language (STL) file. Then the STL file is converted to a g-code, or build-file, for the AM machine software. The g-code file is then sent to the printer and the machine executes the code to fabricate the designed part. Insitu-quality, machine, and overall equipment effectiveness (OEE) data is generated while the print is in progress. The inspection data is then sent to quality engineering and a data lake for analysis. A parallel data transfer updates records of job completion along with initial quality buyoff. The post operations for removal from the build plate and other surface finish and cleanup processes ensue. Lastly, the appropriate labeling and packaging is set up to buy off and move the part to its destination.

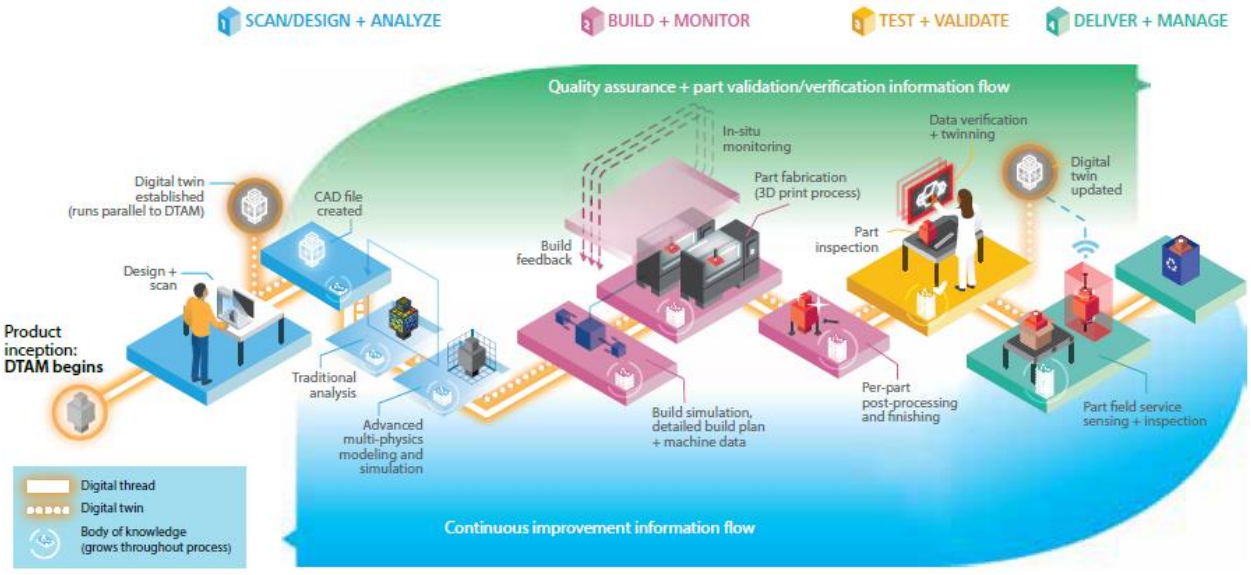


Figure 2.1 AM Digital thread and digital twin depiction (Trouton, Vitale, & Killmeyer, 2016)

The manufacturing process can stand alone with basic paper communication. However, to get the maximum efficiency, the digital thread must be completed so full automation is possible. Figure 2.1 gives a high-level view of the digital thread with the related file types and data. Each colored section corresponds to the "Scan/Design + Analyze", "Build + Monitor", "Test + Validate", and "Deliver + Manage" section of Figure 2.1. The "Build + Monitor" section is a data-intensive section worth focusing on. The section not only encompasses the standard numerical code (NC) execution but also new real-time inspection data. The post-processing status information is a typical manual input now. However, the implications are that robots will be able to replace the human labor.

The AM processes and the potential data outputs were fully researched through personal experience in hands-on aerospace AM and information technology work. Further experience was obtained through the MITxPro *Additive Manufacturing for Innovative Design and Production* course. Scholarly articles, pertaining to industry best practices, added to the overall concepts proposed. The findings revealed that each machine vendor will vary on the input file types and the types of output information. A complete analysis will be completed utilizing data from a set of EOS M290 Direct Metal Laser Sintering (DMLS) machines. Figure 2.2 depicts the full system with the critical EOS software used to collect optical tomography (OT) and melt pool (MP) data.

Figure 2.2 EOS M290 DMLS (EOS M 290, n.d.)

Optical tomography technology captures near-infrared images of the laser-to-metal power heat during a 3D print (EOS, 2017). Melt pool technology captures the light emission of the instant pool of melting metal powder (EOS, n.d.). Together, the two technologies produce detailed image and sensor data necessary for real-time certification. The metrology and inspection data at every approximate thirty-micron layer thickness during fabrication will eventually eliminate the need for post-fabrication inspection.

The proposed methodology will be carried forward as a standard for all advanced manufacturing communications. While metal and polymer processes differ, the abundance of data from DMLS will serve as a comprehensive benchmark for the needed systems.

2.2 CIAN Alignment

Confidentiality, integrity, availability, and non-repudiation are the foundation to cybersecurity. Additive manufacturing (AM) is a core cyber-physical system component of the future automated manufacturing environment (Yampolskiy, et al., 2018, p. 431). Due to popularity, AM is a prime target for cyber criminals seeking to find new gains in this highly connected factory component.

Cryptography dates to roughly 4,000 BC with Egyptian hieroglyphs. The Jews of ancient times also used a cypher form called Atbash. A very interesting form of cryptography was used in Sparta. Inscribed letters on a strip of leather which, when wrapped around the exact diameter rod, revealed the aligned, hidden message (Shcherban, 2018). The need to hide messages has been a military need since nations have warred against each other. The basic fact is ciphers will eventually be broken, so new and better methods must be continually developed.

2.3 Understanding Blockchain Technology

Blockchain, in summary, is a decentralized, distributed digital ledger. The sequential and public transactions are made in bitcoin or another cryptocurrency (Judmayer, Stifter, Krombholz, & Weippl, 2017). The founder of Bitcoin, Nakamoto, originally defined it as the "aggregation and agreement on transactions in an immutable ledger" (Judmayer, Stifter, Krombholz, & Weippl, 2017, p. 19). Figure 2.3 shows the specifics of the transaction as detailed by GAO, et al.

(2018). A block contains a transaction ID (TXID) and the public key of owner one. A hash is generated to act as a finger print to the block, then the signature of owner zero is placed. The private and public key of owner one is used to sign and verify transaction two. The process then starts over with owner two and the blocks and chains form the blockchain.

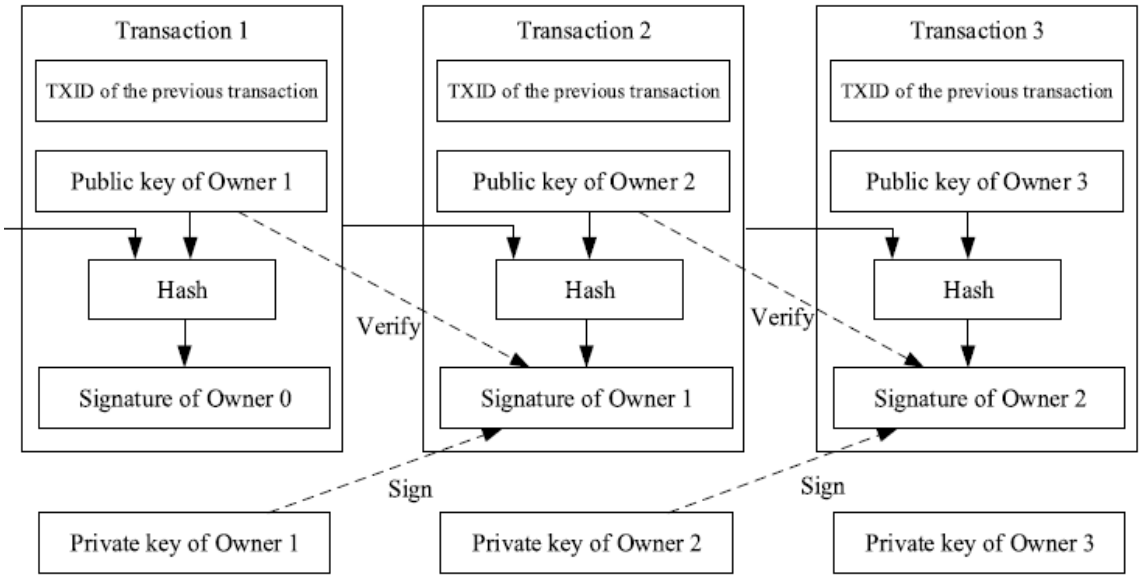


Figure 2.3 Transaction in Bitcoin based on blockchain (GAO, et al., 2018, p. 27207)

Decentralized means the ledger is not in one location like an accountant's ledger. Instead, the information on the transaction is distributed to multiple nodes. The "miners" use their computing power to run a set of algorithms. The process then ensures the validity of the chain of blocks or transactions. A miner is a person who uses their computing power to validate the chain. Payment is expected for doing the work validating the chain's integrity. One of the main keys to this method is that the record can only be appended to. No deletions of previous records can occur. Assurance is made that no fraudulent transactions are inserted (Judmayer, Stifter, Krombholz, & Weippl, 2017, p. 24). For an internal decentralized network, the structure concerning payment for the work, or Bitcoin, for validating the ledger, is unnecessary. The computing equipment is paid for by the employer, and the employees time is already accounted for.

The popularity since the 2008-2009 introduction of Bitcoin, the original blockchain, has increased dramatically to 2,510 as of this writing (All Cryptocurrencies, 2018). A greater percentage of them are derivatives of the original Bitcoin algorithm. However, a portion of them

are now focused on proof-of-work (PoW) methodologies (Judmayer, Stifter, Krombholz, & Weippl, 2017, p. 17).

Blockchain, or cryptocurrency, is a highly researched capability to hold to the CIA framework for security. The quantity of information for one 3D part will be amassed for a valuable biproduct of the manufactured item. Nothing speaks to optimization better than the ability to use a wasted output to bring more value than the part itself. The blockchain methods will be used and combined with robust security methods for a complete end-to-end process flow. Figure 2.4 depicts how blockchain, cryptography, and object storage work together for a cybersecure 3D printing paradigm.

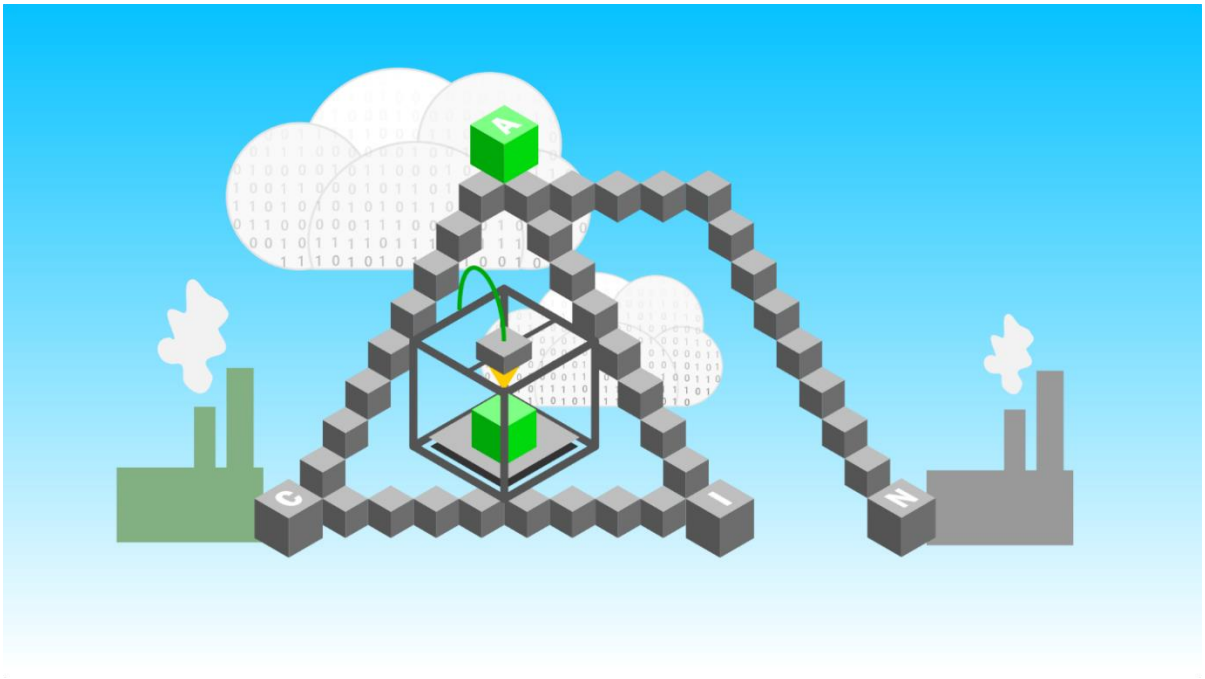


Figure 2.4 CIAN concise depiction for insourced and outsourced 3D printing

The 3D printer in the center is producing the data which is confirmed in the blocks. The source manufacturing company is in green. Confidentiality, integrity, availability, and non-repudiation are key factors in the chain. The clouds represent the object storage methodology. Lastly, the factory on the right represents an external supplier or partner company still being connected to the company's blockchain.

Process knowledge, investigation of cybersecurity best practices, and a review of the latest pertinent technologies will be combined for a final solution. Figure 2.5, on page 24, diagrams a

deeper-level procedure starting from the computer (#1). The process then moves to the metal 3D printer (#2). The detailed ledger is then communicated back to the computer (#3). The blockchain then picks up the ledger through the decentralized processing and databases. Lastly, when the printing process is fully validated, the supplier will be able to access the pertinent singular file (#5). The supplier's work will also be logged to the blockchain and visible to all nodes in the chain. The recommendation will be that only one designee from each internal department is assigned to at 2 blockchains maximum. The need is to keep processing overhead low. Otherwise, normal work being done on the personal computers will be negatively affected.

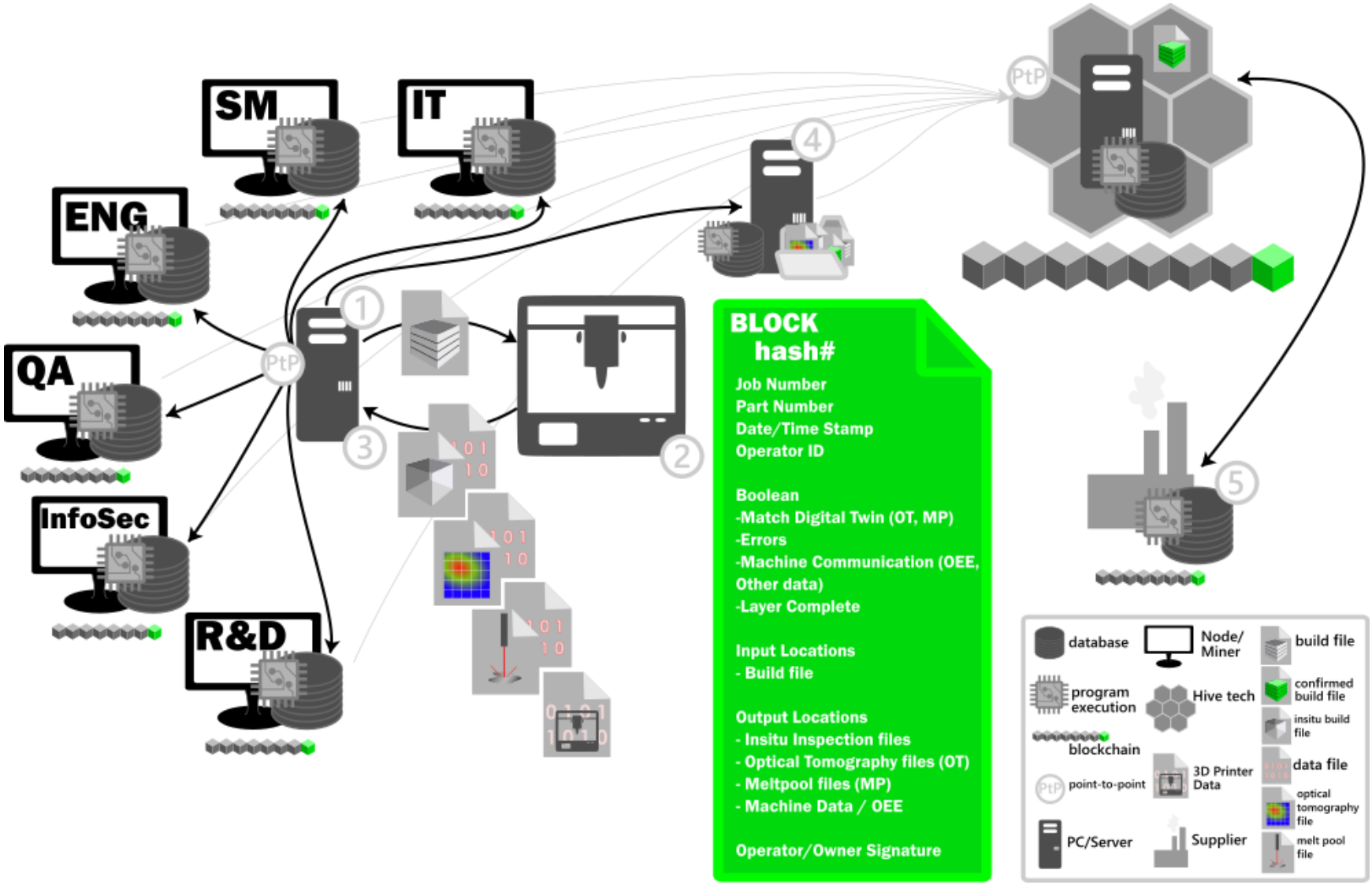


Figure 2.5 Full Detailed Blockchain PoMW Concept

Before the first process flow step is addressed, the computer, or front-end PC (FEPC), function needs to be understood. The FEPC is equipped with two or more network cards which allow two-way communication with the company local area network (LAN). Two-way communication with the 3D printer is also established with another network card. A standard network security configuration is used to isolate the 3D printer. Intellectual property theft or machine process sabotage is prevented since it is on its own local area network (Yampolskiy, et al., 2018, p. 8). However, due to the need to enable the digital thread, campus security firewalls are allowing dedicated devices to connect to the intranet. The information is then available to any other device in the intranet. The reported infrastructure configuration is a key component to enabling the blockchain.

The FEPC will act when the original STL file is transferred to it from a configuration management software on the LAN. Either an operator or an automated program will transform the STL file in to a proprietary build file. A numeric code (NC) build file is created by algorithmically slicing the geometry in to 2D layers and composing the layers together. The first PoMW block is placed in the chain which immediately appears in the register for the LAN-connected nodes. From this point forward, the chain will be continuously appended to by the point-to-point (PtP) node connections as key jobs complete.

The first step in the flow then will show the computer sending the complete build file to the printer. The file then is placed in a queue for the operator to execute the print job. Software residing on the FEPC obtains feedback for the successful file placement in the print queue. The second PoMW block is then recorded in the chain.

The second step commences the execution of the build file instructions. The procedure begins by evacuating the oxygen and replacing it with argon. Data is being generated to show the percentage of oxygen and pressure in the chamber. The data is important to understand potential anomalies which indicate a maximum threshold of oxygen in the system. Once the build process commences the following files and data are generated: optical tomography (OT), melt pool (MP). Also, pre and post powder re-coater pictures are taken. Dozens of machine parameters output data, and machine state data is communicated (running, errors, not running, etc.). Ideally, the live stream of this data is available for immediate reporting. There will be cases where 3D printer companies keep this information proprietary or hard to access in a real-time manner. The

cases will be assessed on a vendor-by-vendor basis for enhancement agreements or application program interface (API) documentation for internal development.

The third step will be to manually or automatically move the raw data files and images to the intelligent repository (#4). Further analysis and required certification will be documented. The blockchain will have already accounted for the files if the real-time process is possible. If not, this will be the time the file information is captured and registered. Importantly, the locations of the files must be tracked in the ledger for full accounting. The files will move to multiple locations due to the massive size on the order of three to six terabytes (TB) per job. Current network and storage technologies cannot support such multi-terabyte sets of data. The blockchain ledger is then a timely technology for PoMW manufacturing jobs.

Throughout the entire process, a knowledge base will form about the parts in the job. The PtP network of nodes will communicate correct and secure blocks of 3D printing information for this knowledge base. Between steps four and five, the Hive technology is storing and maintaining integrity to ensure a process hardened build file. Related certification data will also be packaged together with it. The package will be available for continued insourced work or communicated outside the company firewall to a supplier (#5). Either the internal or external recipient of the complete build package cannot proceed without complying with the blockchain software installation. The installation of the software is the contractual acceptance of becoming a node in the blockchain with full accountability throughout the process. The engineering-owning company will want to confirm and license to very specific devices to decrease the chances of malicious block insertions.

2.4 File Storage Options

Block, object, and file-based storage options yield differences for managing the multiple types of files, sizes, frequency read or written to. Object storage is meant for unstructured data and keeps extended metadata object files in a flat structure. Files are not accessed in the same way within folders as compared to commonly used file systems. Instead, a web interface utilizing representational state transfer (REST) and simple object access protocol (SOAP) over hypertext transfer protocol (http) is used (Rouse, object storage, 2017). A drawback to object storage is the speed of reading and writing data is not as efficient as block storage. Also, it is not meant for data which will be re-written to continuously or in real time.

The benefits of object storage fit the multiple interrelated files case. The files need to be associated together from different processes at different times. Another worthy note is that there is no need for a database in this structure. Instead, files have metadata applied to them and are searched and retrieved based on that information. The object file and the actual file will share matching unique identifiers for association and limitless meta data application.

Wu (2017) gave a detailed explanation of structured (database schema) verses unstructured data (object storage). If business requirements mandate a set of data is organized for very specific output results, a structured database schema is needed. However, a NoSQL database can avoid the database administrator limitations to add or modify attributes of a database instance (p. 8). Wei-ping, Ming-xin, & Huan (2011) explained, a SQL relational database consists of tables with primary and foreign keys to relate the tables together. A NoSQL, like a MongoDB, uses JSON objects to store data or pointers to other data (p. 303). Figure 2.6 depicts the differences between the two structures with example metal additive manufacturing data.

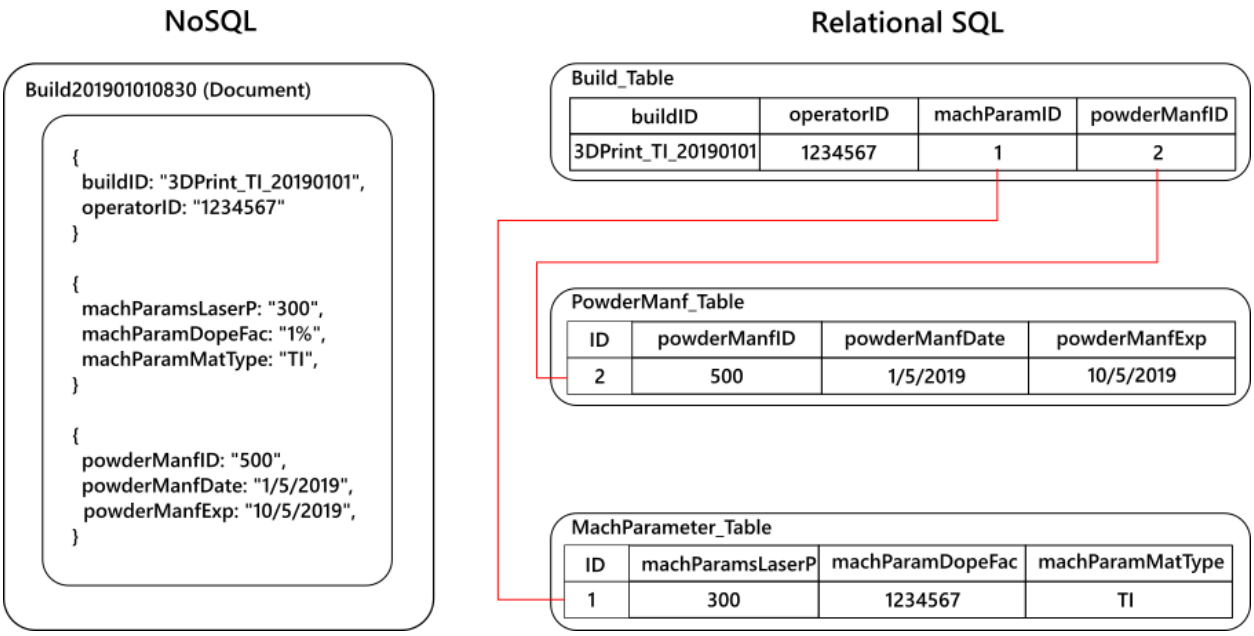


Figure 2.6 NoSQL compared to Relational SQL Database

The NoSQL MongoDB file is attached to the original file as associated, extended metadata. The files are then broken into shards and distributed to multiple storage devices. The unique ID associated to the files, and meta-data, enable a web-interface to be used to search and

retrieve the files. Object storage is meant for files that don't change continuously. If changes are made continuously and modified by more than one person, results containing fragments of the changes are possible.

Object-based storage was reviewed to understand the comparison with standard relational database methodologies as multi-terabytes of data are accumulated over time. One understanding of current and potential future storage methodologies aid in the solution generation process. The horizon of advanced manufacturing capabilities will quickly overwhelm current computing infrastructures as companies continue to gain value from the data. If scalability is not planned for, security gaps can widen.

2.5 AM Attack Taxonomies

Two main categories of attacks exist for additive manufacturing but do not exclude other manufacturing processes. Direct theft of technical data is one category. Hackers can infiltrate a corporate network and steal specific data. The ACAD/Medre worm is one example of a method for theft. The malware was able to steal tens of thousands of AutoCAD™ files from a company in Peru (ESET, 2017). Theft can also occur by direct or outsourced employees of a company. Trust is a difficult value to manage since circumstances with people can change over time. The belief that data is safe on the internal network can lead to weak points in security (Dibrov, 2017, p. 3).

Another category is machine sabotage "generally require[ing] alteration of data, process, and products" (Yampolskiy, et al., 2018, p. 435). The notorious Stuxnet worm is a prime example of the complex nature of targeted malicious programs. The aim was to slowly dismantle the Iranian uranium purification process. The worm was able to manipulate the centrifuge speed and pressure release valves. Machine status was hijacked to hide the tampering of the programmable logic controllers (PLCs). Slowing, speeding up, and holding on to pressure eventually disabled roughly 1,000 centrifuges (Loukas, 2015, p. 128).

Within the two categories there are myriad different ways data and machines are compromised. Yampolskiy, et al. (2018) dive in to the detailed AM attack taxonomies by analyzing how attacks are made along with the properties of the various attacks (p. 435). However, to organize the analysis, the team developed a framework to simplify the taxonomy development (Figure 2.7).

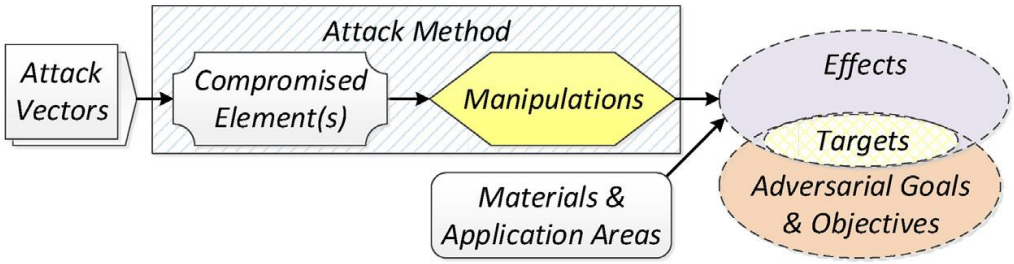


Figure 2.7 AM Attack Taxonomy Framework (Yampolskiy, et al., 2018, p. 434)

The figure just above is comprised of terms requiring definition. Attack vectors, as defined by Souppaya & Scarfone (2016), are "segment[s] of the entire pathway that an attack uses to access a vulnerability" (p. 5). Essentially, it is the method a hacker uses to gain access to networks or computers. A malware payload is then delivered once the vector is successful. One analogy for attack vectors is a guided missile where the payload is the warhead at the tip (Rouse, Attack Vector, 2012). Souppaya & Scarfone (2016) went on to detail further examples of attack vectors:

- Malicious web page content (content) downloaded from a web site (source) by a vulnerable web browser (processor);
- A malicious email attachment (content) in an email client (source) rendered by a vulnerable helper application (processor);
- A malicious email attachment (content) downloaded from an email server (source) to a vulnerable email client (processor);
- A network service with inherent vulnerabilities (processor) used maliciously (content) by an external endpoint (source);
- Social engineering-based conversation (content) performed by phone from a human attacker (source) to get a username and password from a vulnerable user (processor);
- Stolen user credentials (content) typed in by an attacker (source) to a web interface for an enterprise authentication system (processor);
- Personal information about a user harvested from social media (content) entered into a password reset website by an attacker (source) to reset a password by taking advantage of weak password reset processes (processor). (p. 10)

Since computers run numerically controlled machines, an AM machine is a prime target. Compromised elements are any machine, programmable logic controller (PLC), software, firmware, sensor, or network hardware the payload is delivered to. Manipulations are the specific changes made to the compromised elements. Examples are settings changes, code changes, file replacements, sending false positive results to status collections, or changing motor speeds. Materials for AM, according to the Wohlers Report, are contained in two major categories: plastics and metals (Yampolskiy, et al., 2016). The application areas are the things the materials are used for: such as aerospace parts, shoes, etc. Effects are simply the outcomes of the malicious manipulation. Lastly, by tying the effects to the adversarial goals & objectives of the hacker, a target is identified.

A prime example of a successful cyber-physical system attack was the Stuxnet malware on the Iranian uranium enrichment centrifuge system. A direct mapping to the Attack Taxonomy framework (Figure 2.7) is made. See Figure 2.8 for a visual diagram regarding the Stuxnet attack flow.

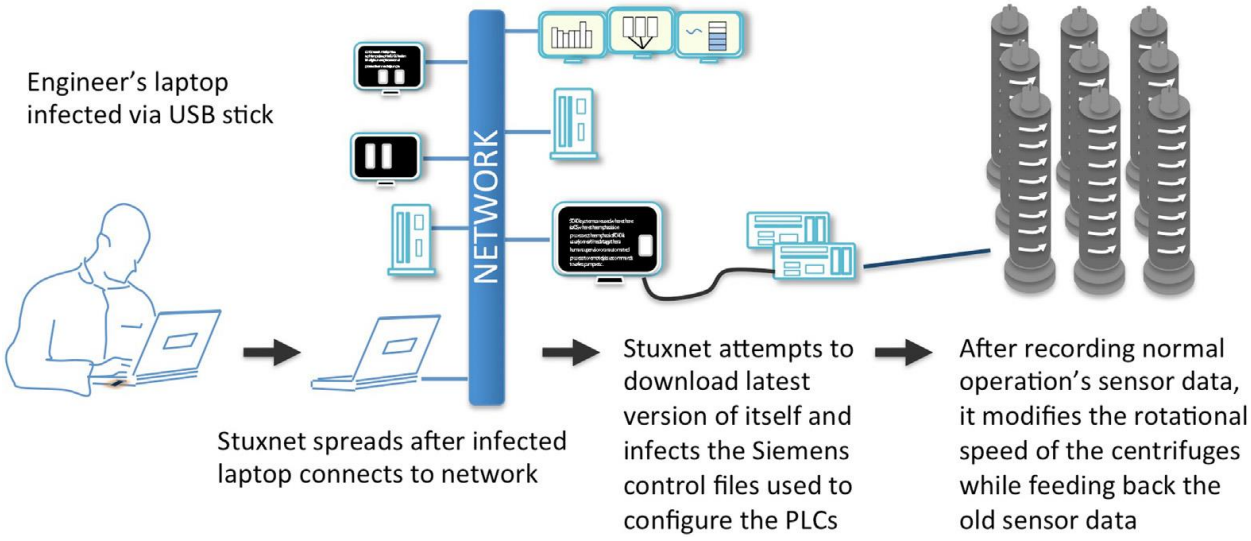


Figure 2.8 Stuxnet exploit diagram (Loukas, 2015, p. 127)

Loukas (2015) gave a thorough analysis of the attack. The attack vector was a thumb drive (or USB stick) where the payload was the malware. Examples of the compromised elements were source laptops, shared printers on the network, Siemens S7-417 PLC controllers, and Siemens S7-315 PLC controllers. Further examples were rotors, valves, sensors, and destination computers. Manipulations were to install the malware program at the controller computer and

adjust the speeds of the controllers. Causing sensors to misread, display the false reading to the operator, and prevent pressure valves from opening were additional manipulations. The materials were un-enriched uranium with the application area of a nuclear weapon. The effects were false readouts of sensor data, speeding up and slowing down the centrifuges. The adversarial goal & objective was to stop the enrichment of uranium by destroying the centrifuges. The target was the centrifuges themselves (p. 122).

The objective, destroying centrifuges at Natanz, Iran, was successful. However, Loukas (2015) concludes that the impact was less successful since the machines were antiquated and prone to breakdown anyhow. Decades of machine repairs is the reason for the Iranians' inadequate nuclear weapons development . However, due to the ability of the virus to reach out to the internet and replicate itself, another 100,000 systems were infected (Loukas, 2015, p. 127).

Yampolskiy, et al. (2018) distinguished why additive manufacturing is unlike traditional numeric control fabrication when considering security compromises. Both device types utilize a machine instruction file to manipulate an end-effector to fabricate a part. However, there are twenty-four fundamental differences which set the technologies apart. Source material, as one example, is compromised more readily due to the local material recycling systems. Manipulations of machine processes, like laser power configurations, can affect a part's fatigue life as well (p. 454). A more complete list of attack taxonomies on AM are provided with additional detail in chapter three.

2.6 Cybercrime Costs to Industry

The costs for cybercrime against United States companies is ever increasing. The Council of Economic Advisers , issuing body (2018) state, "malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016" (p. 2). The council goes on to say that lax protection against cybercrimes leads to under-investments in cybersecurity, especially by the private sector. Figure 2.9 charts the calculations of the percent of industry reported breaches compared to the percentage of 2016 gross domestic product (GDP).

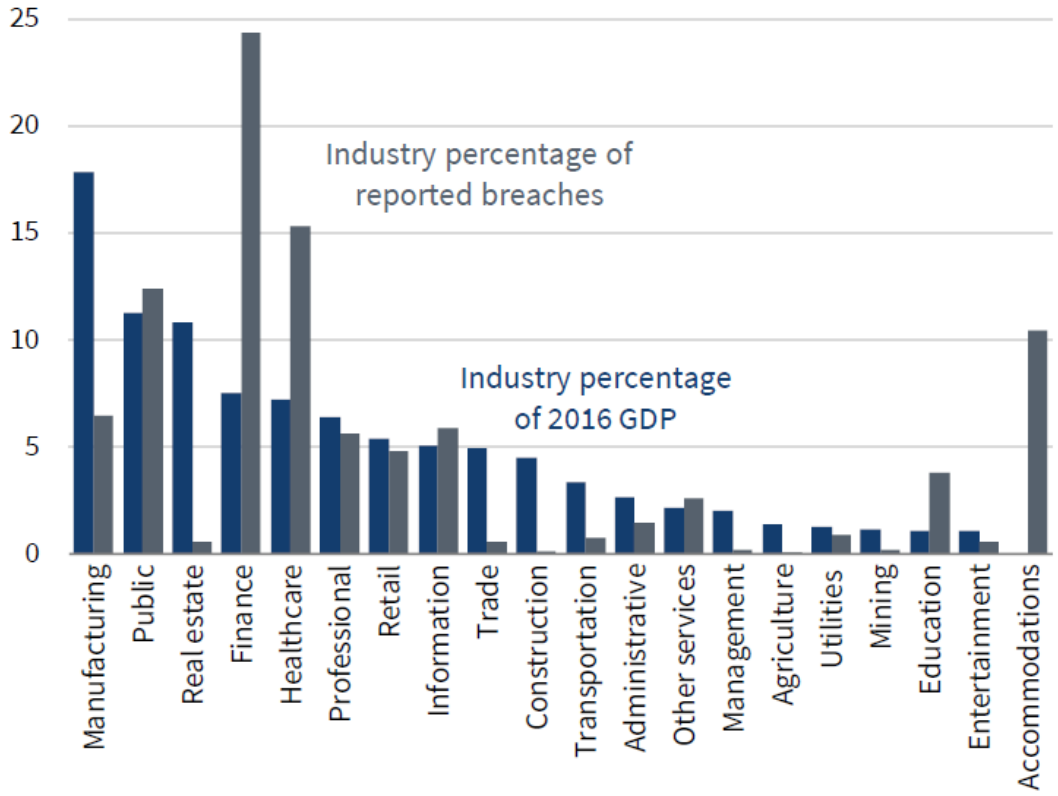


Figure 2.9 Distribution of Security Breaches by Industry - Percentage of 2016 GDP and 2016 Reported Breaches (Council of Economic Advisers , issuing body, 2018, p. 21)

The above chart reveals that education, healthcare, and finance have a higher percentage of breaches compared to their percent of the GDP. However, the focus of this project is on the far-left manufacturing industry with the highest GDP percentage. The reported breaches are close to the professional and information industry percentages. Importantly, a breach is a confirmed, unintentional disclosure of information to a malicious party. A security incident, however, is a compromise of the CIA triad (Council of Economic Advisers , issuing body, 2018, p. 21). The terminology matters when deciphering actual breaches which result in lost intellectual property.

The Council of Economic Advisers (2018) goes on to prove that the costliest type of malicious cyber activity is IP theft. Metrics were gathered against a sample set of 290 security breach events, and the average loss was $498 million per cyberattack. The impact cost was based on the company stock price during a seven-day window after the cyber event was disclosed (p. 9).

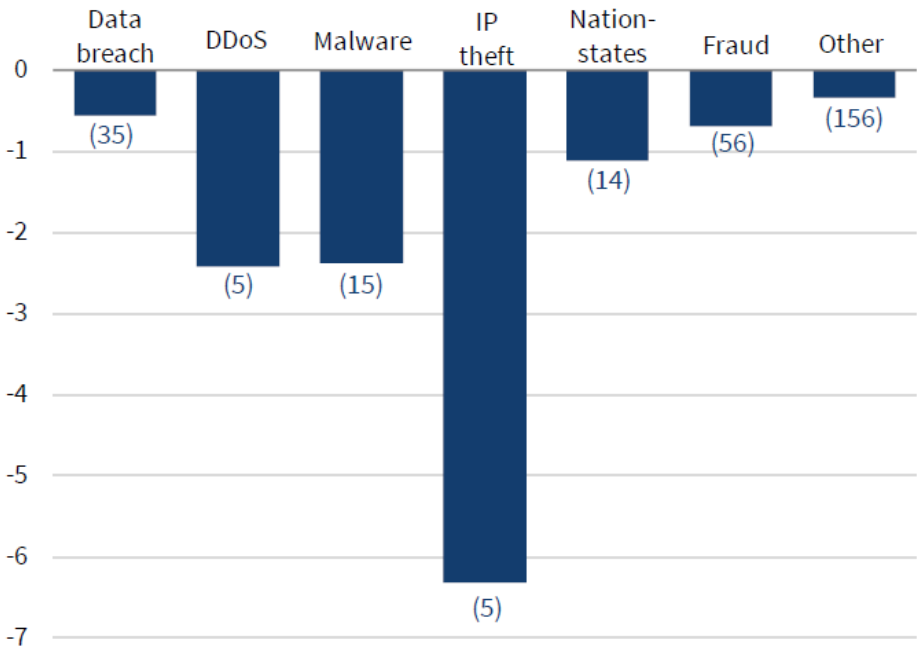


Figure 2.10 "Cumulative Abnormal Return by Type of Adverse Cyber Event" (Council of Economic Advisers , issuing body, 2018, p. 13)

The above figure shows the percentage of negative cumulative abnormal returns for a given category of cybersecurity breach. Market perception of company value, as a result of IP theft, is a 36% more damaging category than the next highest. The sample size, in parentheses, for this result is low; but, the severity of the abnormal drop in market returns gives the score credence.

Lastly, this chapter revealed the extensive investigations made by the Council of Economic advisors. Their findings from market analysis have been used to guide decisions in private and government sectors. Cybercrime is on the rise, and IP is a very costly target.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Problem Statement Overview and Project Direction

A single additive manufacturing (AM) build instruction file holds the complete instructions on how to manufacture an object as good as the original. The need to protect the files from cybersecurity threats is paramount to the success of engineering companies (Chen, Mac, & Gupta, 2017, p. 183). Intellectual property security must be established on a part or build-by-build basis with cybersecurity compliance measures accounting for known attack taxonomies.

Due to the increasingly advanced cyberattack methods, blockchain technology has immerged in response. Being in tandem with other technologies, it ensures confidentiality through the latest cryptography best practices. Assurance of integrity is made through an append-only ledger, and non-repudiation through smart contracts. According to the International Law Review (2018), "smart contracts, though in a different form from traditional written contracts, still memorialize agreements between counterparties" (p. 1). Newer file storage capabilities, like object storage, satisfy the availability requirement as data quantities increase. By methodically combining the technologies and accounting for known and possible attack vectors, the cybersecurity best practice will be satisfied.

3.2 Methodology for Data Collection

Blockchain technology, whether open sourced or vendor developed, is optimally useful when trust is in question. Weber, et al. (2016) go on to say "the described lack-of-trust problem can be addressed with novel blockchain technology" (p. 330). A fully isolated, meaning off the network, manufacturing environment is perceived safe. However, a malicious actor can utilize a thumb drive or temporarily connect an isolated environment to the network. Systems safe from cyber-attacks today are not necessarily safe tomorrow as machines are connected to the network to create smarter factories. Gilchrist (2016) casts the vision for Industry 4.0 stating, "in this transformation, sensors, machines, workpieces, and IT systems will be connected along the value chain beyond a single enterprise (p. 4)".

The Project Management Institute (2017) demonstrated an example risk breakdown structure (RBS) describing sources of project risk. From the levels of breakdown, the second

level describes technical risk, management risk, commercial risk, and external risk. The third tier breaks the bigger categories down. For technical risk, this project focused on technical processes, technology, and technical interfaces. Management risk focus objectives were operations management and resourcing. The commercial risk category identified contractual terms and conditions, internal procurement, suppliers and vendors, subcontracts, and partnerships/joint ventures. Lastly, external risks had a focus from the subcategories of site/facilities, competition, and reputation (p. 406). See Table 3.1 for a concise view of the RBS.

Table 3.1 Customized Extract Risk Breakdown Structure (RBS) (Project Management Institute, 2017, p. 406)

RBS Level 0	RBS Level 1	RBS Level 2
0. All sources of project risk	1. Technical Risk	1.1 Technical Processes 1.2 Technology 1.3 Technical Interfaces 1.4 Technical Data
	2. Management Risk	2.1 Operations Management 2.2 Resourcing
	3. Commercial Risk	3.1 Contractual terms & conditions 3.2 Internal procurement 3.3 Suppliers & Vendors 3.4 Subcontracts 3.5 Partnerships/Joint ventures
	4. External Risk	4.1 Site /Facilities 4.2 Competition 4.3 Reputation

The resultant possibilities for compromised security lead to the need for a comprehensive mapping of multiple variables to assess the risk. Research in to the possible attack taxonomies guides the population of the table along with expert feedback through interviews (see Table 3.2 on page 36). A full reference to all taxonomies from Yampolskiy, et al. (2018) is available in APPENDIX A. Larger views of the tree structure are available in the subsequent pages in the appendix. The full list of the twenty-four attack vectors used in the survey are listed in APPENDIX C.

Table 3.2 Example Survey Matrix

ID	*1*
Taxonomy	*Theft of Technical Data*
Actor	*Machine Operator*
Attack Vector	*Virus on thumb drive (USB drive)*
Compromised Elements	*Thumb drive, Windows 7 or 10 OS, Windows file system*
Target	*Object Specification (Build File)*
Method	*Theft*
Risk Category (from RBS)	*1.4 Technical Data*
Risk Detail	*File stolen and replaced with manipulated file*
Action / Blockchain Opportunity	*Activity logging on thumb drive insertion; record unauthorized devices; develop a reporting mechanism for a machine controller blockchain compliance ledger*
Probability (1 – low, 5 – high)	*4*
Impact (1 – low, 5 – high)	*5*
Blockchain Opportunity (Yes/No)?	*Yes*
If No, expert opinion	

The tabulation served as a means for detailing the potential IP escape through common workday events as well as outside attacks. The focus was on intellectual property theft. The results were identification of threats, the associated risk, and the reasoning against a potential blockchain solution if one existed. The best practice will continue beyond this study with communication to cyber security experts, technology experts, and blockchain architects.

The experts being surveyed were given a standard scale to understand the context of the probability and impact scores. The authors from the Project Management Institute (2017) gave an exemplary model for defining scales for risk assessment. Table 3.3, on page 37, defines a scale with the probability and impact against three project objectives.

Table 3.3 PMBOK Example of Definitions for Probability and Impacts (Project Management Institute, 2017, p. 407)

SCALE	PROBABILITY	+/− IMPACT ON PROJECT OBJECTIVES		
		TIME	COST	QUALITY
Very High	>70%	>6 months	>$5M	Very significant impact on overall functionality
High	51-70%	3-6 months	$1M-$5M	Significant impact on overall functionality
Medium	31-50%	1-3 months	$501K-$1M	Some impact in key functional areas
Low	11-30%	1-4 weeks	$100K-$500K	Minor impact on overall functionality
Very Low	1-10%	1 week	<$100K	Minor impact on secondary functions
Nil	<1%	No change	No change	No change in functionality

The scale has six levels and gives percentage probabilities. The possible impacts on time, cost, and quality are given in their own related scales. The methodology for this project took advantage of this prescribed structure with slight modifications. Investigation in to cybercrime costs from section 2.6 were utilized to populate the cost scoring factors (see Table 3.4).

Table 3.4 Scale for Risk Scoring

Scale	Probability	Negative Impacts Due to Stolen Intellectual Property
		Cost
5 – Very high	>70%	≥ $500 million
4 – High	51-70%	$100 - $499 million
3 – Medium	31-50%	$1 – 99 million
2 – Low	11-30%	$501 - 999 K
1 – Very Low	1-10%	≤ $500 K

The cost range was also determined by the measurable cost reactions corporations took when cybersecurity breaches occur. The Council of Economic Advisers , issuing body (2018) listed “expenditures on forensics, cybersecurity improvements, data restoration, legal fees, and the like” (p. 8) as easily observable costs. If a 500 employee or greater company must make major changes in its cybersecurity infrastructure, it is implied a breach has occurred.

Visual aids helped the survey participant to understand the problem space more thoroughly. Common understanding on right and left-brain strengths prove individuals tend toward textual or visual understanding. Seeing the attack vectors in tandem with the detailed text

from the survey gave the participant a well-rounded understanding of the problem space (see Figure 3.1, on page 39). Both the scoring criteria and the attack vector visual diagram were provided as a handout for the participant to use throughout the process (see APPENDIX B. on page 65).

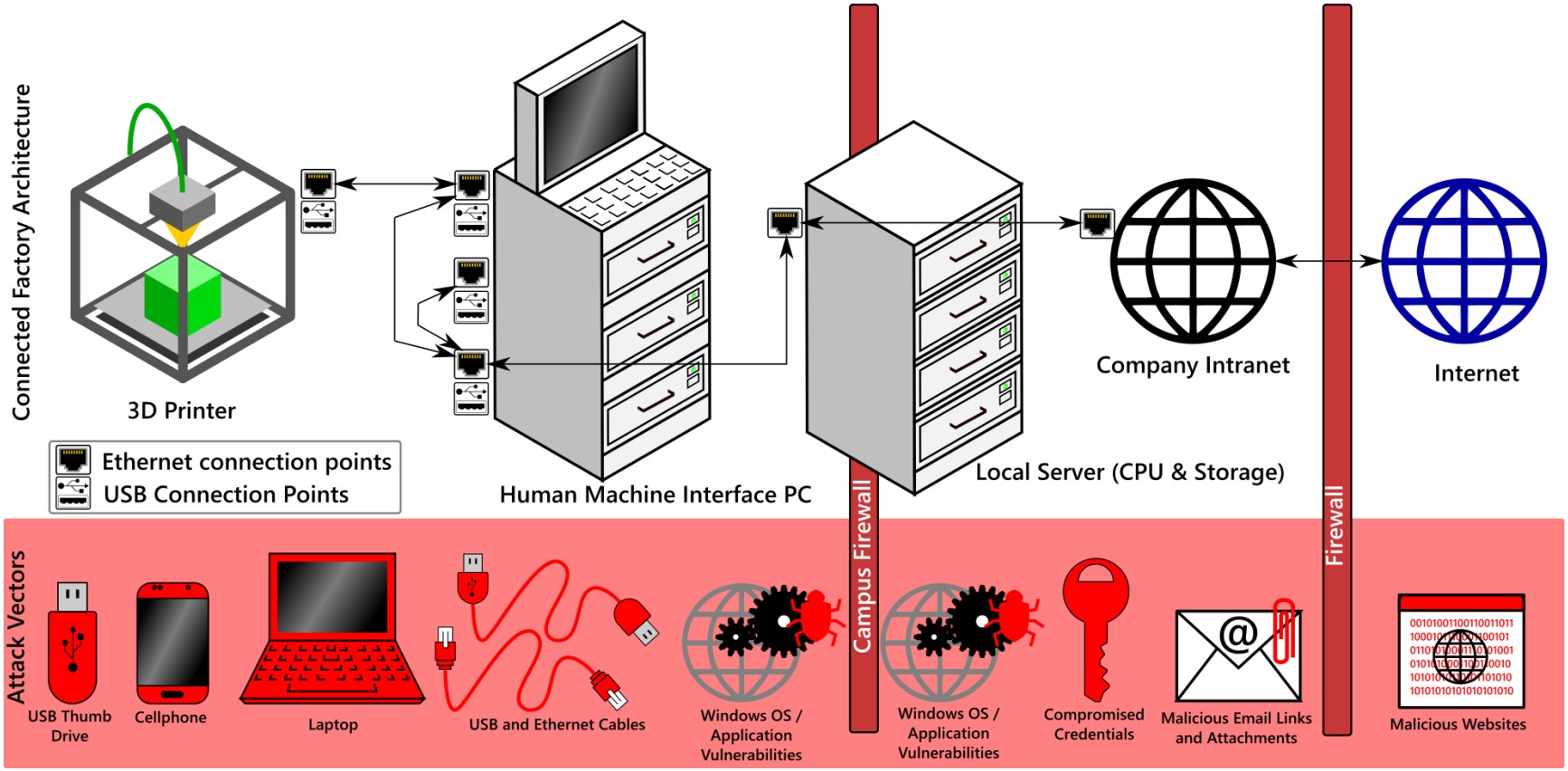


Figure 3.1 Connected Factory Architecture and Attack Vector Diagram

3.3 Survey Questions

The purpose of the survey questions was to marry the scholarly framework with expert experience and opinions. The following questions were standard for each expert to answer once each risk item was reviewed from the survey Excel (Version 15.0.5093.1001; Microsoft, 2013) file:

Given a blockchain solution is in place:

1. What would you rank the probability of the attack occurring? (1 – Low, 5 – High)
2. What would you rank the impact of the attack occurring? (1 – Low, 5 – High)
3. Do you agree the risk will be mitigated with blockchain technology? (1 – Yes, 0 – No)
4. If question 3 answer was no, what alternative technology opportunity can you recommend for mitigating the risk?

If new attack vectors were created, the experts were given another chance to rank the new items in a follow-on interview. Questions one through three were repeated for each new item. Due to the complex nature of the blockchain technology, a brief overview from section 2.3 was given prior to the survey. The intention was to set the expectation and properly guide the survey responses within the scope of the project.

A survey handout was given to each survey participant for ready reference through the scoring process. The RBS table was also provided alongside for clear understanding of the stated risk and how the categorization fits. See APPENDIX B. for the handout.

The survey process, in summary, was as follows:

1. Give introduction to the reason for the study and the benefits to the company for the interviewees' participation
2. Give brief overview of the blockchain technology to fill any knowledge gaps the interviewee has
3. Ask the participant to make their handout visible throughout the interview.
4. Interviewer reads each attack vector item to explain the who, what, how, why, potential risk, and blockchain opportunity.
5. Ask the participant to give a score for Probability and Impact based on the scoring criteria. The participant will be given a maximum of 1 minute for each survey item. If

questions arise, the question may be written down for review after the survey. The intention is to prevent bias during the scoring.

6. After the survey is complete, the risk matrix will be shown as a visual for discussion on the further questions. At this time, the interviewee will be given a chance to add additional attack vectors deemed important. Process steps four through six will then be repeated for the new items.

3.4 Assumptions

The chosen experts were assumed to have enough knowledge from their own studies and professions to accurately score each attack taxonomy. The expected knowledge needed to include costs associated with cybersecurity breaches, known use cases, current related technology, and related future technology. Authors from the Project Management Institute (2017) stated, "Expertise should be considered from individuals or groups with specialized knowledge of similar projects or business areas" (p. 414). Another assumption was the time to collect the information was enough for a proper scoring and average. The final assumption was the study was valuable to the target company. The results help make appropriate decisions on the proper amount of capital to invest in developing the next cybersecurity solution.

3.5 Limitations and Delimitations

The foundation of this study was based on a qualitative measure of risk based on probability and impact per risk identified. Interviewee risk bias was an unavoidable factor. "Risk perception introduces bias into the assessment of identified risks, so attention should be paid to identifying bias and correcting for it" (Project Management Institute, 2017, p. 420). Extensive psychological studies have been done on managing risk attitudes to gain understanding for why certain people make risk decisions. However, due to the smaller number of survey participants, risk attitudes will not be managed.

3.6 Statistical Method Definitions and Appropriateness

Diez, Barr, & Cetinkaya-Rundel (2015) defined "The probability of an outcome is the proportion of times the outcome would occur if we observed the random process an infinite

number of times" (p. 77). The Council of Economic Advisers , issuing body (2018) claimed that insurance companies can run the proper quantitative statistical analysis because of their close relationships with companies (p. 34). However, the unbiased, proprietary information is not available to the public. As a result, probabilistic analysis must be conducted based on public announcements and stock price fluctuations. Another indicator of the higher probability of attacks is the announced expenditures and increased investment in cybersecurity measures. Between 2010-2012, $24.8 billion was spent globally on antivirus and other cleanup and defense technologies. The market is expected to grow to $128 billion by 2020 (Council of Economic Advisers , issuing body, 2018, p. 35).

The probability and impact qualitative analysis was appropriate for this project due to the subjective scoring from experts. Expectations of increasing numbers of cyberattacks lead to the need to assess the risk of not taking the proper preventative measures. The methodology from section 3.2 accounts for proper project management risk assessment and aimed at obtaining the least biased response from interviewees.

Figure 3.2,Figure 3.2 Probability and Impact Risk Matrix Example gives a simplified visual representation of the collected data. Only the attack vectors residing in the upper right half were considered for a future development (cells 5,2; 5,3; 5,4; 5,5; 4,3; 4,4; 4,5; 3,4; 3,5; 2,5). Then, of that quadrant, only those items where the blockchain opportunity question is marked with a "Yes" were reviewed further. The highest priority use cases were revealed by summing the probability and impact scores from each participant for each attack vector.

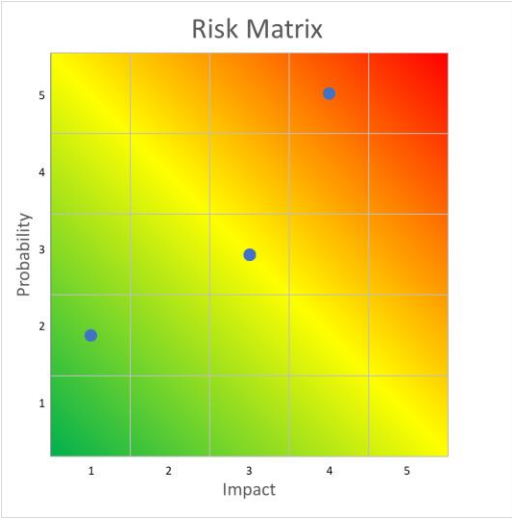


Figure 3.2 Probability and Impact Risk Matrix Example Created in Excel (Version 15.0.5093.1001; Microsoft, 2013)

3.7 Sample Size determination

There were two samples sizes in this study: number of attack vectors and the number of experts to interview. Twenty-four attack vectors were determined from scholarly articles. The number of experts was determined by known available experts which would accept an interview in a two-and-a-half-week timespan. The estimate was four experts: one expert in AM technology, one in blockchain technology, one in infrastructure technology, and one in blockchain architecture.

3.8 Tools Utilized

Excel (Version 15.0.5093.1001; Microsoft, 2013) was the primary tool used for communication, data collection, and results calculations. The tool was chosen due to license availability, common use by all experts, ease of data formatting, and built in calculation features. The results were exported to a Sharepoint (Version 2013; Microsoft, 2013) web interface for reporting within the company. Word (Version 15.0.5093.1001; Microsoft, 2013) was used to design the handout each expert will use for reference when scoring.

3.9 Return on Investment

Cost is associated with the software development costs to create and maintain a blockchain solution against cyberattacks. Estimations for what constitutes a full development team must be taken in to account due to unforeseen budgetary leniencies or restrictions. Assumption was made for a team of six: one manager, one project manager, one architect, and three developers. The Bureau of Labor Statistics (2018) provides a survey for employer cost for employee compensation. The following pertinent details are for the assumed team (see extracted subset in Table 3.5 on page 44).

Table 3.5 Private Industry Workers, Full-Time by Occupational Group: Employer Costs Per Hours Worked for Employee Compensation (Employer Burden Rate)

Occupational Group	Year	Month	Cost per hour worked	Cited page reference
Management, professional, and related occupations	2018	Sept.	$63.57	p. 516
Professional and Related Occupations	2018	Sept.	$58.21	p. 522
All Full-Time Workers	2018	Sept.	$40.18	p. 514

For the team of six, based on the table above, the total burden rate is $63.57/hr (manager) + 116.42/hr (project manager, architect) + 120.54 (three developers) = $300.53\hr. Given an additional full-time technical support cost for a minimum of a year, the full burden rate is $340.71. A one-time cost of the Engineering Technology master's program is added to the estimation (see Table 3.6).

Table 3.6 Total first year cost breakdown

Manager	2 professionals	3 developers	1 Tech Support	One-time costs	Total first year cost
$63.57	$116.42	$120.54	$40.18	$25,000	$733,677

Subsequent years for continued support ideally drop down to one part-time (25%) manager. Reduction to one part-time (25%) technical support can also be expected for a total burden rate of $103.75/hr ($53,950/yr). The average cost of a breach due to a cyberattack, based on numbers from 2016-2017 ranges from $21 million to $498 million. The cost to the company occurs in only seven days from the date of the breach announcement (Council of Economic Advisers , issuing body, 2018, p. 9). Taking the first year of development added to five years of support amounts to $1.003 million. However, preventing a single breach of intellectual properly will save $497 million. If accounting for the loss of company reputation, the company will lose millions more in lost revenues from potential future sales.

The return on investment was calculated for a single software development project. Subsequent developments are expected to be increments utilizing the base code formulated for the solution. As a result, the costs are lower for each subsequent development. Estimations are for new developments not existing costs a corporation has already spent if pursuing a blockchain solution.

CHAPTER 4. RESULTS

4.1 Introduction

A single additive manufacturing (AM) build instruction file holds the complete instructions on how to manufacture an object as good as the original. The need to protect the files from cybersecurity threats is paramount to the success of engineering companies (Chen, Mac, & Gupta, 2017, p. 183). Intellectual property security must be established on a part or build-by-build basis with cybersecurity compliance measures accounting for known attack taxonomies. Intellectual property theft taxonomies include side-channel methods using sound and heat signature sensors from smart phones to re-produce part geometry. Cybersecurity attacks with thumb drives and malicious code also threaten the protection of sensitive AM files.

Due to the increasingly advanced cyberattack methods, blockchain technology has immerged as one response. Working in tandem with cybersecurity technologies, it ensures confidentiality through the latest cryptography best practices. Assurance of integrity is made through an append-only ledger, and non-repudiation through smart contracts.

The contents of Chapter Four cover the research question, goal of the research, findings and statistical discussion related to the findings. The expectation from the assumptions and limitations, sections 3.4 and 3.5, were accurate during the actual data collection. Detail from the following sections explains the results of the data.

4.2 Research Question and Goal

The research question was: Given a developed blockchain solution is in place, what are the probabilities and impacts of additive manufacturing intellectual property theft for each potential attack vector? Twenty-four attack vectors and their associated risks were listed, and each received its own probability and impact scoring by each surveyed expert. A brief introduction was given so the participant fully understood what was expected of them. One-hour sessions were dedicated to each participant to allow enough time to complete the survey.

The overall goal of the survey was to determine if every possible attack vector had been addressed and considered by the expert. If an attack had not been considered, the scoring would be high on probability and impact. If an attack had been considered and planned for, the

probability and impact would be lower. Lastly, if the listed attacks were not extensive enough, the expert was asked to input items of their own. The results from all four surveys were expected to reveal three top attack vectors, thus exposing priority security gaps to fill. Microsoft Excel (Version 15.0.5093.1001; Microsoft, 2013) was used as the primary calculation and analysis tool. Reasonings for the tool included ease of formula creation, ease of relationship mapping, ease of data formatting, and chart creation ability.

4.3 Findings

The risk matrix formed a five-by-five grid with the lowest probability and impact appearing in the lower left quadrant. The highest probably and impact appear in the upper right quadrant. Summing the probability and impact gives a score along the negative sloping diagonal bands (See Figure 4.1).

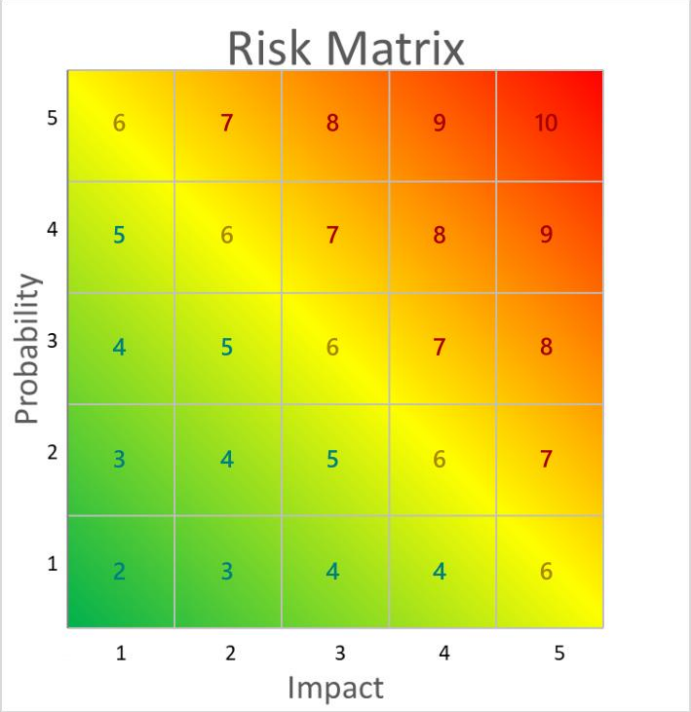


Figure 4.1 Probability and Impact Scoring Example

The Purdue ENGT507-Collaborative Leadership and Agile Strategy course detailed the formulation of the matrix in Figure 4.1 above. Dr. Hutchison said, “the combined weight of all of those judgments will lead the group in the right direction” (Explore | The Big Easy, 2017). Out of

the four surveyed, a total individual risk score of eight was the highest recorded. Two was the lowest score recorded. Only scores of seven or higher were considered candidate attack vectors for further prioritization and development work. No single attack vector was agreed to be in the seven or higher scoring range by all four participants. One vector was agreed to be high risk and priority by three of the participants, however. The item was ID #9, which is the vector "Malicious code injected in firmware update." The blockchain chief architect noted the vector was already being considered. The other three participants, independently, did not think so.

Table 4.1, on page 48, gives more detail on the participants and their highest scored attack vectors. A relationship was also made between the highest ranked and commonality with the other participants.

Table 4.1 Detailed Score with Attack Vectors Showing Most Agreement (green) and Agreement by at Least Two Participants (yellow), generated in Excel (Version 15.0.5093.1001; Microsoft, 2013)

Participant	Attack Vector ID	Attack Vector	Total Score
Chief AM Architect	4	Thumb drive to transfer tampered build file	7
	5	License Dongle	8
	8	Malicious code injected in software update	7
	9	Malicious code injected in **firmware** update	7
	24	Malicious DRM removal application	8
Blockchain Expert	1	Thumb drive to transfer tampered build file	7
	9	Malicious code injected in **firmware** update	7
	23	Malicious contract operator	7
Computing Infrastructure Expert	5	License Dongle	7
	8	Malicious code injected in software update	7
	9	Malicious code injected in **firmware** update	7
	10	Malicious code injected in software update	7
	11	Malicious code injected in firmware update	7
	15	Malicious webpage installs a virus on PC.	7
	19	Laser Scanner	7
	20	Laser Scanner	7
	21	Stolen metallic powder composition reports	7
	22	Malicious subcontract operator	7
	23	Malicious contract operator	8
	24	Malicious DRM removal application	8
Chief Blockchain Architect	22	Malicious subcontract operator	6

The Chief Blockchain Architect technically did not have a score above six. However, since it was the highest score for this participant, it was included.

Table 4.1, above on page 48, also helped to produce the prioritization list of attack vectors to develop against. First in the priority is ID #9, "Malicious code injected at firmware update" due to the majority consensus. The next priority, ID #24 "Malicious DRM removal" is set by the highest scored consensus by two participants. The third priority is a tie between ID #5 "License Dongle" and ID #23 "Malicious Contract operator."

The overall score was calculated for the probability and impact score. Each survey participant's overall impressions of all the attack vector possibilities are graphed as percentages in Figure 4.2. If all twenty-four attack vectors received a probability score of one, the lowest total score was twenty-four. If all twenty-four attack vectors received a probability score of five, the highest total score was 120. The range was 96. All raw survey data are viewable in APPENDIX D.

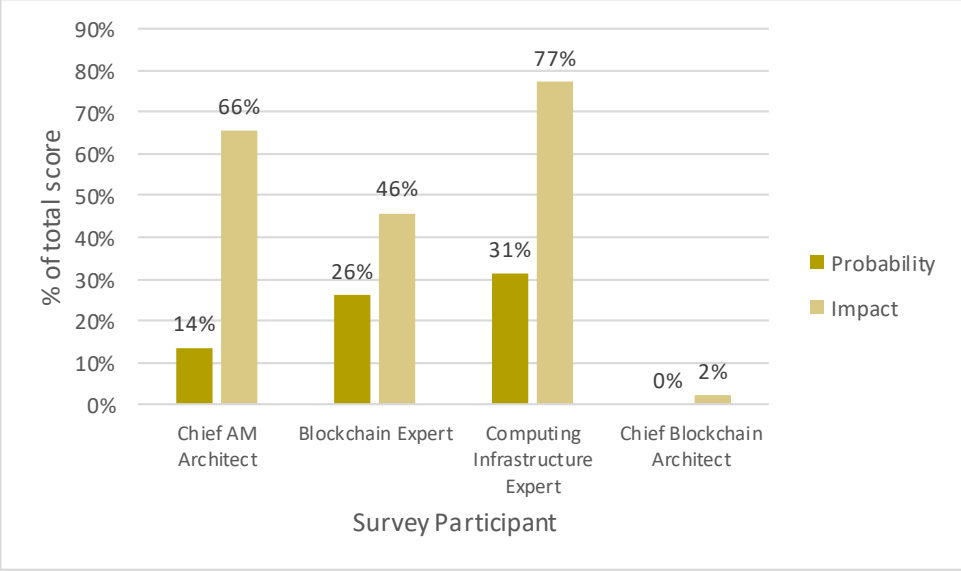


Figure 4.2 Total Scores of Percent Probability and Percent Impact for Each Surveyed Participant, generated in Excel (Version 15.0.5093.1001; Microsoft, 2013)

Figure 4.2, above, shows the perception of attacks being successful, given blockchain technology is in place, is low to medium (reference Table 3.4 for the scale). The Chief Blockchain Architect was so sure of the technology that the scores show no possibility of an attack getting through. The impact if an attack was successful while using a blockchain implementation is perceived to be medium to very high ($99 million to > $500 million) by three of the participants.

One additional finding was that none of the participants added additional risk items in scope of the project. The authors of Guide to the Project Management Body of Knowledge stated, "The meeting may also identify addtional risks during the discussion, and these should be recorded for analysis" (p. 426). The data collection objectives were stated repeatedly in each session with each survey participant to obtain additional risk items. An opportunity to give feedback, days after the initial meeting, was also communicated.

4.4 Statistical Discussion

The authors of *Guide to the Project Management Body of knowledge* said, "Differences in the levels of probability and impact perceived by stakeholders are to be expected, and such differences should be explored" (p. 423). The focus of the analysis was to find the similarities; however, differences are also worth exploring in the future.

Due to the qualitative risk assessment, standard distribution statistical methods could not be observed. The use of the probability and impact matrix is a satisfactory method to "numerically analyze the combined effect of identified individual project risks…" (Project Management Institute, 2017, p. 428). The authors of *Guide to the Project Management Body of knowledge* state:

> "An organization can assess a risk separately for each objective (e.g., cost, time, and scope) by having a separate probability and impact matrix for each. Alternatively, it may develop ways to determine one overall priority level for each risk, either by combining assessment for different objectives, or by taking the highest priority level regardless of which objective is affected" (p. 425).

The analysis method complies with the quoted statement above where assessments were combined for the different objectives. Prioritization was then taken from that assessment by comparing individual risk assessments. The target for the study was AM intellectual property theft, so the theme for each risk attack vector revolved around that target. Combining the results, therefore, offered an accurate overall assessment for risk understanding from each participant.

4.5 Conclusion

The low number of survey participants still yielded a top three priority risk assessment. Surveying more participants undoubtedly solidifies the top priorities for focused continued development work. The fact no other risks were added concludes that enough research was done to assure the participants of a thorough analysis. All participants completed the survey and indicated, except for one participant's single score, all attack vector risks could be mitigated with blockchain. Overall, the scoring data shows blockchain technology is agreed to be a highly secure and accountable method for protecting AM intellectual property. The cost impact is also agreed to be high, meaning between $100-$499 million, if developments cannot prevent the IP theft from occurring.

CHAPTER 5. CONCLUSIONS

5.1 Introduction

Chapter four took the methodology from chapter three and put it in to action through surveying experts. Assessment of the benefits of blockchain technology for use in Additive manufacturing was necessary to understand true cybersecurity protection capabilities. A traditional project management risk assessment, through qualitative analysis of perceived probability and impacts, was the main tool used to collect data. Chapter five summarizes the project, gives conclusions based on the data collection results, and provides recommendations for further development.

5.2 Summary

5.2.1 Additive Manufacturing verses Traditional

Additive manufacturing (AM) has many similarities to traditional numerical code (NC) machining. Machine instruction files, or build instruction files for AM, tell the programmable logic controllers (PLCs) exactly how to behave to create the end-product. NC programmers used to write the machine instructions or g-code by hand, line-by-line. Today, however, computer aided design and computer aided manufacturing (CAD/CAM) software is used to automatically generate the needed information with advanced, machine-specific parameters. The similarities begin to depart from this point.

Industry 4.0 is about using information technology to optimize the supply chain. Data from sensors, cameras, up-stream processes, and down-stream processes all come together to form a digital thread. The thread can describe a product's maturity at any point in time as it moves toward the end-product design intent. The main departure of AM and NC comes with the ability to specifically control material properties as the product is being built. Complexity can be achieved with no tooling or fixture changes, which reduces cost inherent in traditional manufacturing. The reduction in setup time also reduces the overall time to fabricate.

5.2.2 Problem

Combined with all the other data streams, proprietary recipes are formed for every newly created 3D-printable product. The complete recipe is contained in a single build instruction file specific to each printer manufacturer. Protecting the files is the focus as growing network-connected factories become less trusted environments than the traditional isolated machine model.

5.2.3 Solution

Blockchain technology is proposed as a remedy to the trustless environment. Instead of trusting build files and resulting information are protected at every step in the manufacturing process, blockchain automatically confirms security. Confidentiality, integrity, availability, and non-repudiation (CIAN) are the foundations of cybersecurity. Blockchain, a popular technology as of 2008 (Judmayer, Stifter, Krombholz, & Weippl, 2017, p. 1), has spread and been developed to protect data for the financial industry. Now, the technology is beginning to focus on the manufacturing industries to confirm and protect the digital thread.

A survey was given to a set of experts within an aerospace company specializing in AM, computer infrastructure, and blockchain. The overall question to participants was "Given a blockchain solution is in place, what are the probabilities and impacts of intellectual property theft?" Twenty-four potential cybersecurity attack vectors, or methods for attack, with risk statements were given to the participants to score. Both probability and impact receive a score of 1-low to 5-high. The scoring definitions were provided to help associate percent probability and impact costs per attack vector. The overall goal of the survey was to reveal and prioritize AM intellectual property cybersecurity risks for blockchain development. The sub-goal was to ensure all facets of cybersecurity were accounted for in the AM process. Another sub-goal was to validate blockchain as a plausible solution in the manufacturing space verses the common bitcoin space.

The survey results accomplished the main goal and four attack vectors rose to the top for development focus. The vectors, in priority order, are "Malicious code injected at firmware update", "Malicious DRM removal", "License dongle", and "Malicious contract operator." Majority consensus on the first vector was reached mainly because machine firmware is the least controlled technology in the system. Trust is given to machine vendors to provide the firmware

needed for the machines to run properly. When the machine runs properly, focus is diverted to other production needs. The remaining vectors gained consensus from fifty percent of the participants.

5.3 Conclusions

5.3.1 Related Findings from Literature Review

The review of literature covered the AM process, CIAN alignment, blockchain technology, file storage, AM attack taxonomies, and cybercrime costs to industry. A complete grasp on the AM process aided the research in narrowing down the scope to the problem. Focus was placed on the fabrication section of the product lifecycle where the build instruction file and resultant output files were exposed. Other areas of the lifecycle suffer from the risk of intellectual property theft as well. The benefit of this study is that it can be replicated to the other areas for full coverage over time.

Confidentiality, integrity, availability, and non-repudiation (CIAN) are the foundational elements of cybersecurity. The research in to this area served the needs of confirming the blockchain technology adheres to the foundation of security. Scholarly articles, books, and evidence from in-use developments confirm the technology to be a robust solution for cybersecurity. The financial market, with bitcoin, has exploited blockchain capabilities through encryption, a distributed append-only ledger, and smart contracts which covers CIAN. Using blockchain in the same fashion for manufacturing accountability is the focused challenge now. Additive manufacturing, and blockchain reaching maturity in a similar timeframe, provides opportunities for technology growth.

File storage technology was researched to understand how the flow of data would be impacted by cybersecurity attacks. Emphasis was placed on reviewing block verses object-storage. However, attack taxonomy research and resultant, defined attack vectors proved to exclude storage methodologies as a factor for build instruction file cybersecurity. Blockchain technology is focused on identifying files and objects of the system – not managing file movement and attribution. Other developments for secure file transfer and intelligent file fragmentation will need to be used in tandem with blockchain to manage data sets in the manufacturing value stream.

Additive manufacturing attack taxonomies have been identified in the literature to organize the myriad ways technology and data can become compromised. Focus was found to be placed mainly on machine and data manipulations over data theft. The reason was due to the focus on the differences in AM technology over traditional manufacturing processes. However, enough evidence for AM specific data theft, tied with other known cyberattack taxonomies, gave grounds to continue the research direction.

Cybercrime costs to industry were important to understand the relevance of the research currently and in to the coming future. Gale (2017) states, "cost[s] of cyberattacks [are] expected to increase from $3 trillion in 2015 to $6 trillion by 2021" (p. 14). The opportunities for cyber criminals and government organizations increase as software and systems become more complex and difficult to manage. Industry costs due to cyberattacks have been studied by observing publicly held company stock values along with direct surveys. Results of these studies prove which industries are at higher risk and the average cost of a total breach of security. The manufacturing industry reports less breaches than the financial industry. Manufacturing, however, holds the highest gross domestic product value out of all the industries. The data between these two factors points to manufacturing being a major focus for cybercrime despite reported events to the contrary (Bureau of Economic Analysis, Gross Domestic Product, 2018).

5.3.2 Limitations

Conducting interviews in a two-week span amid conflicting schedules was difficult. Business travel, vacations, and other priority work all contributed to delays and requests for research extensions. Difficulty finding people with blockchain expertise in the company also contributed to the small sample of experts to take the developed survey. More time was needed to review companies outside of the target company. Relationships were not established early enough in the process to find the right contacts in those outside companies, however. During the survey, it was difficult to keep participants on track – partly because the decisions took more reasoning and thinking than expected.

Future investigation would benefit with four to six weeks of scheduled survey times. Participants would have the opportunity to communicate with their colleagues and business partners about the study. The communication will help to increase the sample size of participants

and likely gain perspectives outside of the target company. One preparatory meeting before the main survey meeting would keep the survey session moving forward more efficiently. Technical topics, for some, need more thought to give an accurate answer.

5.3.3 Research Methodology and Findings

The methodology for research into blockchain, as a solution for preventing intellectual property theft in additive manufacturing, utilized a project management approach. A risk breakdown structure was defined, and a set of twenty-four attack vectors from research and industry experience were detailed. Attack vector, actor objective, risk detail, action/blockchain opportunity, probability, impact, and blockchain opportunity (yes/no) were the only categories of information seen. Another five categories, used to aid the creation of the 24-risk-item list, were hidden to eliminate clutter, however. The hidden categories were used to make sure there was alignment and accounting for attack targets, attack methods, and the risk breakdown.

The intention behind each of the risk item details was to paint a picture of the scenario. The participant needed to provide a probability and impact scoring from 1-low to 5-high based on the scenarios. The participant was given a handout with scoring criteria. A depiction of the attack vectors in a real-life hardware architecture setup was also given to help the visual learner. The participant was also asked if they thought the risk and opportunity could be solved with blockchain. The input for that data point was a Boolean yes or no. If the answer was no, the risk item was not counted in the data analysis as a priority item for that participant. The excluded item, however, was not excluded for other participants. Expert opinions were collected per risk item to capture a form of feedback for later refinement or addition to the assessment.

Findings from the study were both from communication methods and the actual risk scoring data. One pre-meeting with the chief architect for AM revealed the need for reducing the viewable columns. Showing only what the participant needed for scoring drastically sped up the survey process compared to the pre-meeting attempt. Allowing the participant time to think through the scenario and not interjecting clarifications also helped to establish a consistent scoring cadence. Properly evaluated risks from a larger functional cross-section than just blockchain experts was useful to gauge risk. Full risk assessments from researched attack vectors gave a more wholistic view of the cyberthreats needing solutions.

Findings from the risk scoring data were overwhelmingly in favor of using the blockchain solution. The given perspective was a blockchain solution was in place and the risk event occurred. All four participants believed the probability of a successful cyber-theft was 31 percent or less (3-medium to 2-low probability on the scale). One participant gave a zero percent probability that theft could occur with a blockchain solution in place. The cost impacts, if an AM IP theft was successful, were between 46 to 77 percent (4-high to 5-very high on the scale). The top three priorities, after all data was analyzed, were successfully identified from the correlations of the data.

5.4 Recommendations

5.4.1 Impacts

Information technology is not the only department impacted by AM IP theft. Engineering, business partners, suppliers, customers, and shareholders all feel the ramifications. Opening connections to machine controllers and improperly handling complete build instructions files, creates risk inside and outside a company. Assessing security risks through non-conventional thinking helps to fill security gaps before malicious intents can be fulfilled. Metal 3D printing is becoming a highly competitive market, so more attention is being paid by malicious actors.

Companies bringing capabilities in-house and vertically integrating internally means the company wants total control of the process. Advanced 3D printing benefits, such as newly discovered processes to yield high-strength material properties, are a driving business factor. If the direction is such, then IT needs to meet or exceed internal business expectations to protect with the proper technologies. More risk surveys need to be run and on a regular basis to gauge the movement of internal organizations. The possible gaps open as demands increase.

5.4.2 Cost and ROI

A single reported cybersecurity breach, meaning theft of data, costs a company up to $498 million in reparations and lost stock value. Other than cost, negative impacts on reputation, accelerated by the socially connected world, affects a company through turned down contracts as well. Safety, while not a focus in the research, is also compromised when the stolen data results

in a sub-standard quality product. The fabrication process may not account for less defined attributes needed to create the correct quality product.

The proposal is to form a development team with focus on the top priority risks identified in this study. Section 3.9 brakes down the costs in more detail. Taking, however, the first year of development added to five years of support amounts to $1.003 million. The estimate is based on data from the United States Bureau of Labor Statistics for U.S. workers. The costs would be less if a sourced company was used. The overall return on investment would then be $497 million in the event of a reported breach of cybersecurity. Unreported cases still suffer from millions of dollars in reparation costs and insurance deductibles.

5.4.3 How the Solution Solves the Problem

Gale (2017) states, "According to Cybersecurity Ventures, the annual cost of cyberattacks is expected to increase from $3 trillion in 2015 to $6 trillion by 2021" (p. 14). The doubling of the costs in the trillions over six years reveals the urgent need for protecting intellectual property at all costs. Multi-million-dollar additive manufacturing investments are among the high-risk categories for theft.

Digital manufacturing, of which additive manufacturing is one part, is only increasing in system complexity. To account for all possible cybersecurity breaches leading to theft of intellectual property, full research and risk assessments must be conducted frequently. The practice of auditing the complex systems will keep a vulnerable manufacturing company ahead of the cybercriminals. Companies can no longer afford to wait for negative multi-million-dollar impacts due to cybersecurity compromises in order to improve security infrastructure.

The blockchain solution helps to fill cybersecurity gaps with full considerations in confidentiality, integrity, availability, and non-repudiation. Intricate system designs are only possible if computing automation aids the human. Blockchain, if developed for the specific cybersecurity considerations in additive manufacturing, will protect the valuable data as it traverses the digital thread.

REFERENCE LIST

All Cryptocurrencies. (2018, December 2). *All Cryptocurrencies*. Retrieved December 2, 2018, from Investing.com: https://www.investing.com/crypto/currencies

ASTM. (2015). *ISO/ASTM 52900-15: Standard Terminology for Additive Manufacturing - General Principles - Terminology* (ISO/ASTM 52900:2015(E) ed.). West Conshohocken: ISO.

Bureau of Economic Analysis. (2018, September 6). *Gross Domestic Product*. Retrieved January 27, 2019, from Bureau of Economic Analysis - U.S. Department of Commerce: http://www.bea.gov/resources/learning-center/what-to-know-gdp

Bureau of Economic Analysis. (2018, April). *Gross Domestic Product*. Retrieved January 27, 2019, from The Bureau of Economic Analysis: http://www.bea.gov/sites/default/files/2018-04/GDP-Education-by-BEA.pdf

Chen, F., Mac, G., & Gupta, N. (2017). Security features embedded in computer aided design (CAD) solid models. *ELSEVIER*, 182-194.

Council of Economic Advisers , issuing body. (2018). *The cost of malicious cyber activity to the U.S. economy*. The Council of Economic Advisers, Executive Office of the President of the United States.

Dibrov, Y. (2017). The Internet of Things is Going to Change Everything About Cybersecurity. *Harvard Business Review*, 1-5.

Diez, D. M., Barr, C. D., & Cetinkaya-Rundel, M. (2015). *OpenIntro Statistics* (Third ed.). openintro.org. Retrieved June 24, 2018, from https://www.openintro.org/stat/textbook.php?stat_book=os

EOS. (2017, June 19). *EOS releases EOSTATE Exposure OT: Optical Tomography (OT) for real-time monitoring of metal-based Additive Manufacturing*. Retrieved December 1, 2018, from EOS: https://www.eos.info/press/eos-releases-eostate-exposure-ot-optical-tomography-for-real-time-monitoring-of-metal-based-additive-manufcaturing

EOS. (n.d.). *EOSTATE MeltPool: Real-time process monitoring for EOS M 290*. Retrieved December 1, 2018, from EOS: https://www.eos.info/software/monitoring-software/meltpool-monitoring

EOS M 290. (n.d.). *EOS M 290*. Retrieved December 2, 2018, from eos.info: https://www.eos.info/eos-m290

ESET. (2017). *ACAD/Medre.A 10000's of AutoCAD Designs leaked in suspected industrial espionage*. ESET. Retrieved December 6, 2018, from welivesecurity:

https://www.welivesecurity.com/media_files/white-papers/ESET_ACAD_Medre_A_whitepaper.pdf

Gale, S. (2017). AI vs. Hackers. *PM Network*, 14-15.

GAO, Y.-L., CHEN, X.-B., CHEN, Y.-L., SUN, Y., NIU, X.-X., & YANG, Y.-X. (2018). A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. *IEEE Access, 6*, 27205-27213.

Gilchrist, A. (2016). *Industry 4.0 The Industrial Internet of Things*. New York: Apress. doi:10.1007/978-1-4842-2047-4

Haimes, Y. Y. (2015). *Risk Modeling, Assessment, and Management*. John Wiley & Sons, Incorporated.

Hart, J. (2018, May). MIT Basic AM Cost Model. Cambridge, Massachusetts, United States.

Hartman, P. L., Ogden, J. A., & Hazen, B. T. (2016). Bring it back? An examination of the insourcing decision. *International Journal of Physical Distribution & Logistics Management*, 197-222.

Hirsch, M., Patel, R., Li, W., Guan, G., Leach, R. K., Sharples, S. D., & Clare, A. T. (2017). Assessing the capability of in-situ nondestructive analysis during layer based additive manufacture. *Additive Manufacturing*, 135-142.

Hutcheson, S. (2017, September). *Explore | The Big Easy*. Retrieved March 3, 2019, from MET 581000 - Workshop in MET / ENGT 50700 - Collaborative Leadership & Agile Strategy - Section 01 - Fall II 2017: https://engage.purdue.edu/learn/mod/page/view.php?id=56631

Judmayer, A., Stifter, N., Krombholz, K., & Weippl, E. (2017). *Blocks and Chains, Introduction Introduction to Bitcoin, Cryptocurrencies, and their Consensus Mechanisms*. Morgan & Claypool. doi:10.2200/S00773ED1V01Y201704SPT020

Loukas, G. (2015). *Cyber-Physical Attacks: A Growing Invisible Threat*. Oxford: Elsevier.

Project Management Institute, I. (2017). *Guide to the Project Management Body of Knowledge (PMBOK® Guide)* (6th ed.). Project Management Institute, Inc. (PMI). Retrieved January 20, 2019, from https://app.knovel.com/hotlink/toc/id:kpGPMBKP02/guide-project-management/guide-project-management

Rouse, M. (2012, May). *Attack Vector*. Retrieved from searchsecurity.techtarget.com: https://searchsecurity.techtarget.com/definition/attack-vector

Rouse, M. (2017, January). *object storage*. Retrieved November 8, 2018, from TechTarget: https://searchstorage.techtarget.com/definition/object-storage

Secure Cyberspace. (2018). Retrieved October 18, 2018, from NAE Grand Challenges for Engineering: http://www.engineeringchallenges.org/challenges/cyberspace.aspx

Shcherban, V. (2018). Cryptography and Blockchain. Technics Publications. Retrieved November 4, 2018, from https://www.oreilly.com/library/view/cryptography-and-blockchain/9781634624039/

Smart, N. P. (2018). *Topics in Cryptology – CT-RSA 2018*. San Francisco: Springer.

Souppaya, M., & Scarfone, K. (2016). Guild to Data-Centric Threat Modeling. *NIST Special Publication*, 1-20. Retrieved January 19, 2019, from https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

Straub, J. (2017). A combined system for 3D printing cybersecurity. *SPIE Digital Library* (pp. 102200N-102200N-13). Anaheim: SPIE Commercial. doi:10.1117/12.2264583

The Bureau of Labor Statistics. (2018, September). *Employer Costs for Employee Compenstaion Historical Listing - National Compensation Survey*. Retrieved January 29, 2019, from United Stated Department of Labor - Bureau of Labor Statistics: https://www.bls.gov/web/ecec/ececqrtn.pdf

Trouton, S., Vitale, M., & Killmeyer, J. (2016). 3D Opportunity for blockchain: Additive manufacturing links the digital thread. *Deloitte University Press*, 1-20.

Weber, I., Xu, X., Ponomarev, A., Riveret, R., Governatori, G., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. *Business Process*, 329-347.

Wei-ping, Z., Ming-xin, L., & Huan, C. (2011). Using MongoDB to Implement Textbook Management System instead of MySQL. *Communication Software and Networks (ICCSN)* (pp. 303-305). 2011 IEEE 3rd International Conference.

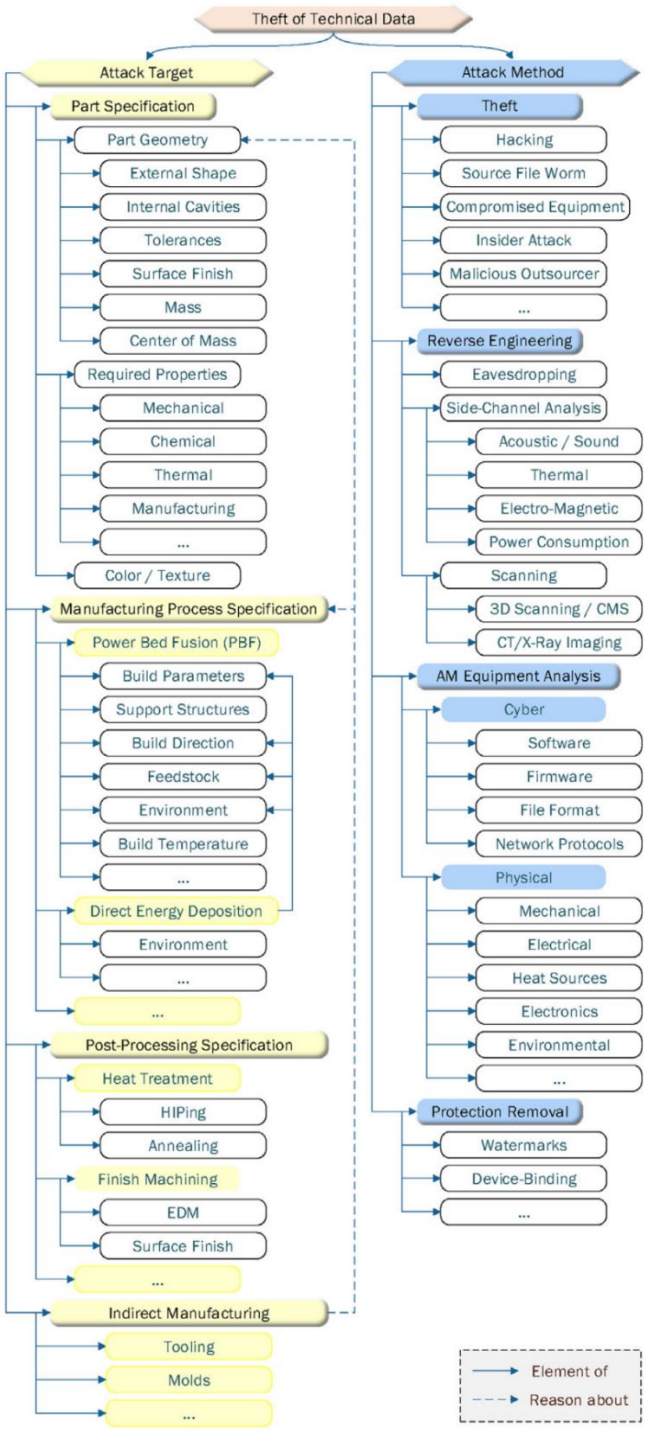
Why blockchain smart contracts matter. (2018). *International Financial Law Review*. Retrieved January 21, 2019, from https://search.proquest.com/docview/2020422359?accountid=13360

Wu, H. (2017). *A Distributed Blockchain Ledger for Supply Chain*. Ann Arbor, MI: ProQuest Dissertations Publishing. Retrieved January 15, 2018, from http://search.proquest.com/docview/1980717693/

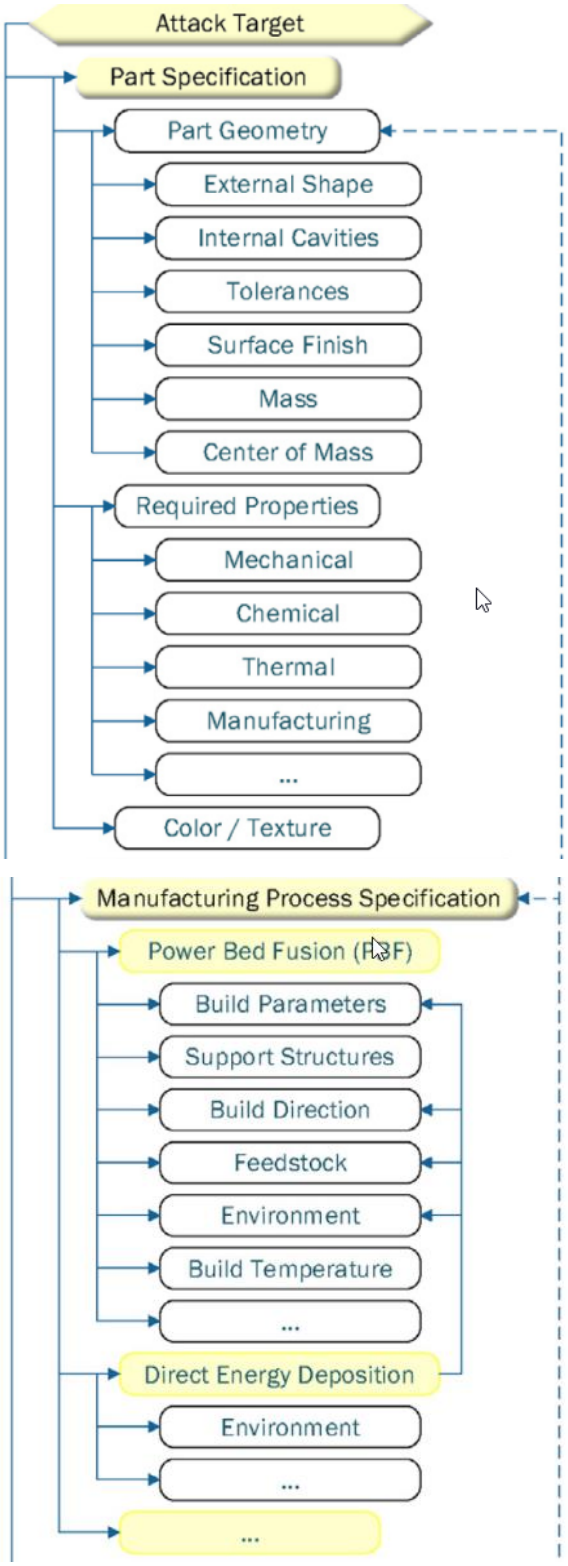
Yampolskiy, M., King, W. E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A., & Elovici, Y. (2018). Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing, 21*, 431-457.

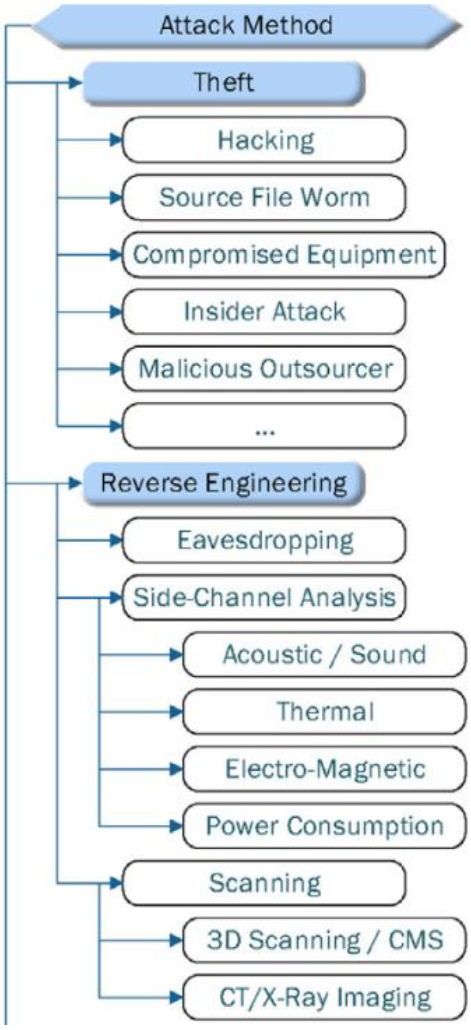
Yampolskiy, M., Skjellum, A., Kretzschmar, M., Overfelt, R. A., Sloan, K. R., & Yasinsac, A. (2016). Using 3D Printers As Weapons. *Elsevier*, 58-71.

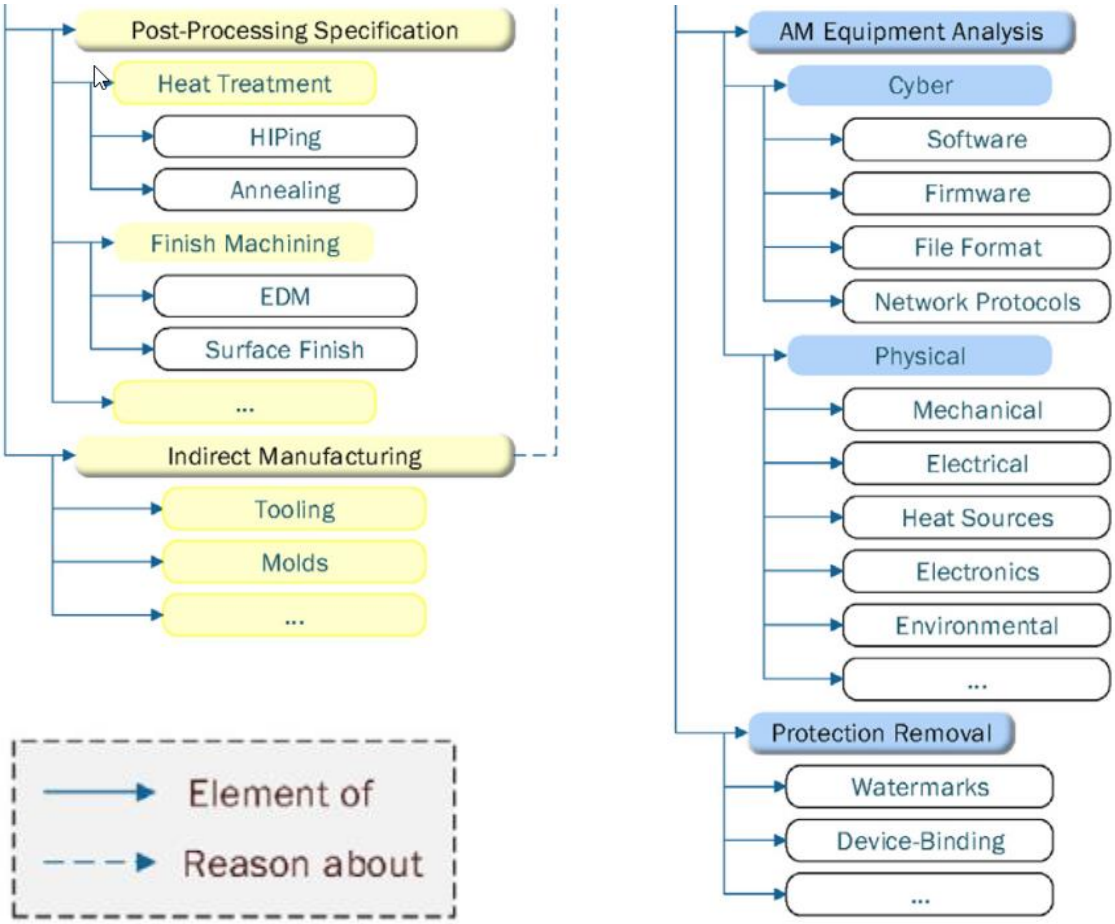
APPENDIX A. AM TECH DATA THEFT ATTACK TAXONOMIES



(Yampolskiy, et al., 2018, p. 436)


Attack Target
Part Specification
Part Geometry
External Shape
Internal Cavities
Tolerances
Surface Finish
Mass
Center of Mass
Required Properties
Mechanical
Chemical
Thermal
Manufacturing
...
Color / Texture
Manufacturing Process Specification
Power Bed Fusion (PBF)
Build Parameters
Support Structures
Build Direction
Feedstock
Environment
Build Temperature
...
Direct Energy Deposition
Environment
...
...


Attack Method
Theft
Hacking
Source File Worm
Compromised Equipment
Insider Attack
Malicious Outsourcer
...
Reverse Engineering
Eavesdropping
Side-Channel Analysis
Acoustic / Sound
Thermal
Electro-Magnetic
Power Consumption
Scanning
3D Scanning / CMS
CT/X-Ray Imaging


Post-Processing Specification
Heat Treatment
HIPing
Annealing
Finish Machining
EDM
Surface Finish
...
Indirect Manufacturing
Tooling
Molds
...
AM Equipment Analysis
Cyber
Software
Firmware
File Format
Network Protocols
Physical
Mechanical
Electrical
Heat Sources
Electronics
Environmental
...
Protection Removal
Watermarks
Device-Binding
...
Element of
Reason about

APPENDIX B. SAMPLE SURVEY HANDOUT/TIPSHEET

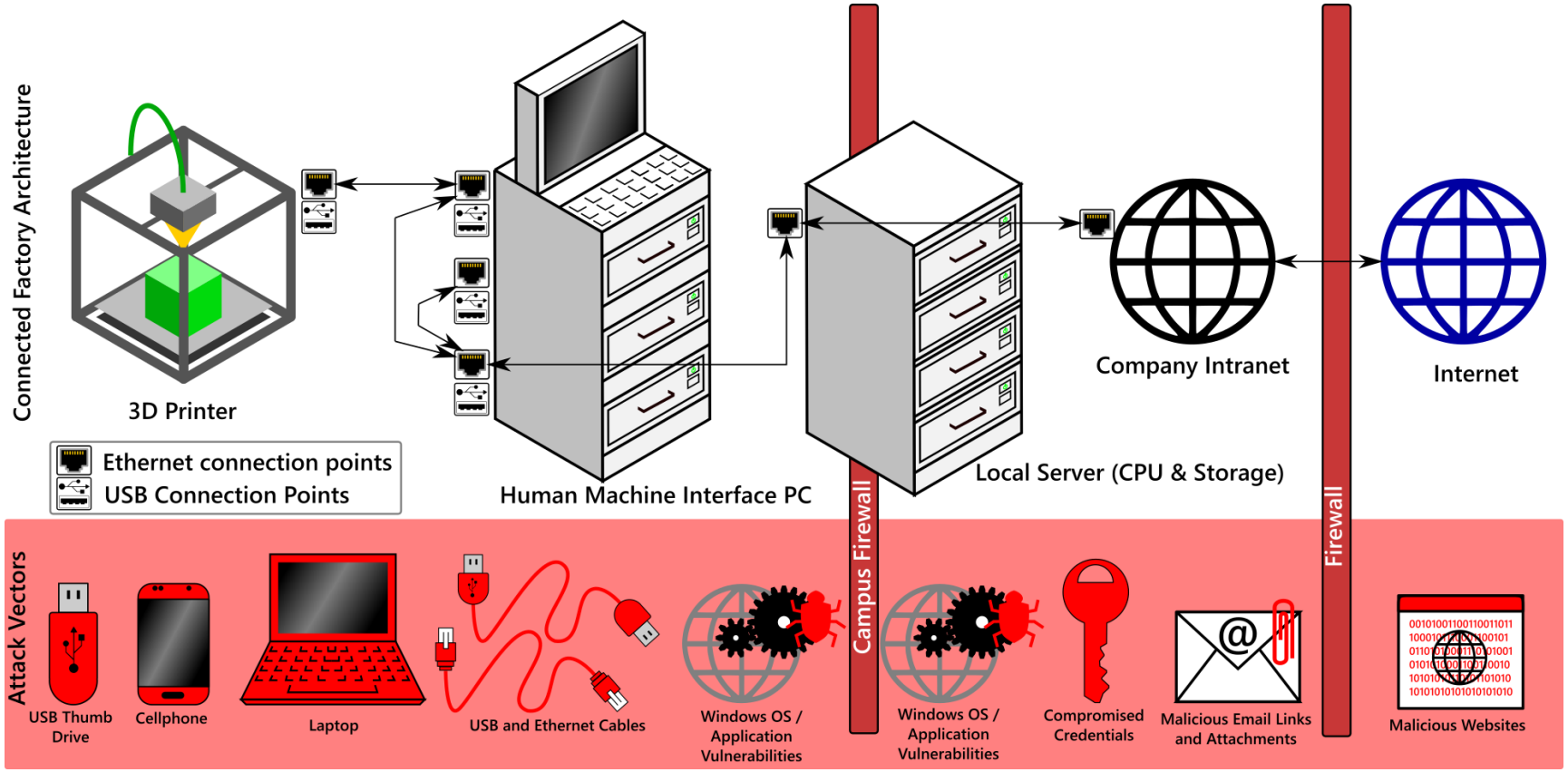
Survey Questions

Given a blockchain solution is in place:

1. What would you rank the probability of the attack occurring? (1 – Low, 5 – High)
2. What would you rank the impact of the attack occurring? (1 – Low, 5 – High)
3. Do you agree the risk will be mitigated with blockchain technology? (1 – Yes, 0 – No)
4. If question 3 answer was no, what alternative technology opportunity can you recommend for mitigating the risk?

Scale	**Probability**	**Negative Impacts Due to Stolen Intellectual Property** **Cost**
5 – Very high	>70%	≥ $500 million
4 – High	51-70%	$100 - $499 million
3 – Medium	31-50%	$1 – 99 million
2 – Low	11-30%	$501 - 999 K
1 – Very Low	1-10%	≤ $500 K

RBS Level 0	RBS Level 1	RBS Level 2
0. All sources of project risk	1. Technical Risk	1.1 Technical Processes 1.2 Technology 1.3 Technical Interfaces
	2. Management Risk	2.1 Operations Management 2.2 Resourcing
	3. Commercial Risk	3.1 Contractual terms & conditions 3.2 Internal procurement 3.3 Suppliers & Vendors 3.4 Subcontracts 3.5 Partnerships/Joint ventures
	4. External Risk	4.1 Site /Facilities 4.2 Competition 4.3 Reputation


Connected Factory Architecture
3D Printer
Ethernet connection points
USB Connection Points
Human Machine Interface PC
Local Server (CPU & Storage)
Company Intranet
Internet
Campus Firewall
Firewall
Attack Vectors
USB Thumb Drive
Cellphone
Laptop
USB and Ethernet Cables
Windows OS / Application Vulnerabilities
Windows OS / Application Vulnerabilities
Compromised Credentials
Malicious Email Links and Attachments
Malicious Websites

APPENDIX C. ATTACK VECTOR SURVEY RISK LIST

ID	Attack Vector	Actor Objective	Risk Detail	Action / Blockchain Opportunity
1	Thumb drive to transfer tampered build file	Inadvertent	Malware installed. If network is completely isolated, malicious code could carry files on/off network when the operator plugs the thumb drive in elsewhere. If target machine is connected, files could be carried through the network.	Activity logging on thumb drive insertion to a factory PC. Record unauthorized devices (meaning not "Data Traveler" devices)
2	Thumb drive to transfer tampered build file	Inadvertent	Malware installed. The malcious code convinces operator that the build file is authentic	Activity logging on thumb drive insertion to a factory PC. Record unauthorized devices (meaning not "Data Traveler" devices). Ledger policy contains known checksum for original released file.
3	Thumb drive to transfer tampered build file	Inadvertent	Malware installed. Lost intellectual property and report of theft reaches the public	Activity logging on thumb drive insertion to a factory PC. Record unauthorized devices (meaning not "Data Traveler" devices)
4	Thumb drive to transfer tampered build file	Inadvertent	Malware installed. The management did not enforce the proper use of IT security standard thumb drive.	Activity logging on thumb drive insertion to a factory PC. Record unauthorized devices (meaning not "Data Traveler" devices). Ledger policy contains field that manager has taken an IT security training.
5	License Dongle	Malicious	Brute force data theft through copying the file. Viewing the existing file will show no tampering since it was just copied	Activity logging on thumb drive insertion to a factory PC. Record unauthorized devices (meaning not "Data Traveler" devices). Windows Event Logs set to trace copy operations.

6	Thumb drive to copy build file	Malicious	Brute force data theft through copying the file. Viewing the existing file will show no tampering since it was just copied	Activity logging on thumb drive insertion to a factory PC. Record unauthorized devices (meaning not "Data Traveler" devices). Windows Event Logs set to trace copy operations.
7	Malware on IT Administrator's laptop	Inadvertent	A compromised IT admin's laptop contains malicious code which replicates itself through the remote desktop connection to the target PC behind the campus firewall to grab target data during the existing connection or the next time the IT admin remotely connects in the future.	IT Admin PCs required to validate on a device security blockchain prior to any remote desktop connecting. Remote desktop software and version.
8	Malicious code injected in software update	Inadvertent	The malicious code targets AM Build files and attempts to break into the internal network to carry the data to the destination	Mandate appscan of all vendor applications. A checksum of the approved software is recorded in the software compliance blockchain confirmed before each print
9	Malicious code injected in **firmware** update	Inadvertent	The malicious code targets AM Build files and attempts to break into the internal network to carry the data to the destination	Mandate appscan of all vendor applications. A checksum of the approved software is recorded in the software compliance blockchain confirmed before each print
10	Malicious code injected in software update	Inadvertent	The malicious code targets part geometry information as a result of inspection scans such as x-ray and attempts to break into the internal network to carry the data to the destination	Mandate appscan of all vendor applications. A checksum of the approved software is recorded in the software compliance blockchain confirmed before each print
11	Malicious code injected in firmware update	Inadvertent	The malicious code targets part geometry information as a result of inspection scans such as x-ray and attempts to break into the internal network to carry the data to the destination	Mandate appscan of all vendor applications. A checksum of the approved software is recorded in the software compliance blockchain confirmed before each print

12	Malware injected after opening malicious email attachment	Inadvertent	The malicious code carries trade secret build file specification information out of the internal network. Competitive methods like fill density, laser patterns, and other settings are shared to the public	In addition to standard cybersecurity best practices, utilize blockchain to ensure checksum change management on the target PDF files, repository webpage, database, and automation application
13	Malware injected after opening malicious email attachment	Inadvertent	The malicious code carries trade secret build file specification information out of the internal network. Competitive methods like fill density, laser patterns, and other settings are shared to the public	In addition to standard cybersecurity best practices, utilize blockchain to ensure checksum change management on the target PDF files, repository webpage, database, and automation application
14	Malware injected after opening malicious email attachment	Inadvertent	The malicious code carries trade secret build file specification information out of the internal network. Competitive methods like fill density, laser patterns, and other settings are shared to the public	In addition to standard cybersecurity best practices, utilize blockchain to ensure checksum change management on the target PDF files, repository webpage, database, and automation application
15	Malicious webpage installs a virus on PC.	Inadvertent	A PDF file disguised as a typical specification document is used as a Trojan to deploy malicious code to retrieve AM Build Files.	In addition to standard cybersecurity best practices, utilize blockchain to ensure change management on the target specification PDF files and their repositories.
16	Malware on cellphone	Malicious	The machine operator cellphone is near the 3D printer through it's process and records transposed data based on motor sounds and magnetic intensity as the metal print head moves in the machine. The method collected enough data to reconstruct the 3D object.	Enable local 4G wireless to control cellular traffic. Utilize a blockchain to track cellphone uploads.
17	Malicious email attachment	Inadvertent	The malicious code carries complete thermal images out of internal network and is used by malicious actor to reproduce the target part	Blockchain to ensure no copies of data are made.

18	Thumb Drive	Malicious	Malicious actor steals machine configuration information which contains the special recipie for fabricating metal titanium parts	Windows audit log activation on file/folder access to configuration location.See Tip for setup
19	Laser Scanner	Malicious	Malicious supplier actor point-cloud scans the part after print to capture the geometry.	Blockchain application installed at the supplier to ensure next steps in the manufacturing process are followed exactly. This includes expected timings for part travel from one post-operation location to another.
20	Laser Scanner	Malicious	Malicious supplier actor point-cloud scans the part after print to capture the geometry.	Blockchain smart contract application installed at the supplier to ensure next steps in the manufacturing process are followed exactly. This includes expected timings for part travel from one post-operation location to another.
21	Stolen metallic powder composition reports	Malicious	A malicious actor steals report information on the exact blends of metallic powder feedstock to sell to a competitor.	Blockchain to track what user exports what reports. Trend analysis will key in on odd behavior for mitigation.
22	Malicious subcontract operator	Malicious	A contractor can subcontract for post-operations without the owning company's awareness. Even post-operations could utilize a build file or 3D geometry for base and support removal.	Enforce blockchain smart contracts. If contracting supplier will most likely subcontract due to their known capabilities, enforce a tracking infrastructure like RFID to track the part through the process.
23	Malicious contract operator	Malicious	Offshore partners have less oversight and are more at risk for malicious actors. X-Ray images, provide very detailed information about the part which can be easily investigated for grain structure to decipher laser and material specifications	Enforce blockchain smart contracts. If contracting supplier will most likely subcontract due to their known capabilities, enforce a tracking infrastructure like RFID to track the part through the process.

24	Malicious DRM removal application	Malicious	The build file could be tampered with to remove unique identifiers on the 3D printed part to prevent ID of the owning organization. Sale of the part to competitors would then go un-noticed.	Blockchain to compare expected to measured micrograin structure physically unclonable function (PUF) which focuses on a regions of interest (ROI) to calculate the 3-demensional mean intercept length to produce a 1 or 0 pass/fail result (Yampolskiy et al., 2018, p. 445)

APPENDIX D. RAW SURVEY DATA

	Chief AM Architect				Blockchain Expert				Infrastructure Expert				Chief Blockchain Architect			
ID	Probability	Impact	Total Score	Blockchain Opportun	Probability	Impact	Total Score (>6)	Blockchain Opportun	Probability	Impact	Total Score (>6)	Blockchain Opportun	Probability	Impact	Total Score	Blockchain Opportuni ty?
1	2	4	6	Yes	4	3	7	Yes	3	3	6	Yes	3	5	8	No
2	2	4	6	Yes	1	5	6	Yes	3	3	6	Yes	1	1	2	Yes
3	2	4	6	Yes	1	3	4	Yes	2	4	6	Yes	1	1	2	Yes
4	2	5	7	Yes	4	2	6	Yes	2	4	6	Yes	1	1	2	Yes
5	3	5	8	Yes	1	1	2	Yes	3	4	7	Yes	1	1	2	Yes
6	1	4	5	Yes	1	1	2	Yes	2	4	6	Yes	1	1	2	Yes
7	2	4	6	Yes	1	3	4	Yes	2	4	6	Yes	1	1	2	Yes
8	2	5	7	Yes	2	4	6	Yes	2	5	7	Yes	1	1	2	Yes
9	2	5	7	Yes	2	5	7	Yes	2	5	7	Yes	1	1	2	Yes
10	1	3	4	Yes	2	3	5	Yes	2	5	7	Yes	1	1	2	Yes
11	1	3	4	Yes	2	4	6	Yes	2	5	7	Yes	1	1	2	Yes
12	1	3	4	Yes	2	1	3	Yes	1	4	5	Yes	1	1	2	Yes
13	1	3	4	Yes	2	1	3	Yes	1	4	5	Yes	1	1	2	Yes
14	1	3	4	Yes	2	1	3	Yes	1	4	5	Yes	1	1	2	Yes
15	1	3	4	Yes	1	4	5	Yes	2	5	7	Yes	1	1	2	Yes
16	2	4	6	Yes	3	2	5	Yes	1	3	4	Yes	1	1	2	Yes
17	1	3	4	Yes	3	3	6	Yes	1	4	5	Yes	1	1	2	Yes
18	2	4	6	Yes	2	3	5	Yes	2	4	6	Yes	1	1	2	Yes
19	1	2	3	Yes	2	4	6	Yes	3	4	7	Yes	1	1	2	Yes
20	1	2	3	Yes	2	4	6	Yes	3	4	7	Yes	1	1	2	Yes
21	1	3	4	Yes	3	3	6	Yes	3	4	7	Yes	1	1	2	Yes
22	1	3	4	Yes	1	1	2	Yes	3	4	7	Yes	2	4	6	Yes
23	1	3	4	Yes	4	3	7	Yes	4	4	8	Yes	1	1	2	Yes
24	3	5	8	Yes	1	4	5	Yes	4	4	8	Yes	1	1	2	Yes

Individual Totals	37	87			49	68			54	98			24	26		
Highest Probability	5, **24**				1,4 ,23				23, **24**				22			
Highest Impacts		4, 5, 8, **9**, 24				2,**9**				8, **9**, 10 ,1 1, 15				22		
Highest Totals (right-most quad)			4,5, 8,**9**, 24				1,**9** ,23				5,8, **9**,10 ,11, 15,1 9,20 ,21, **22**,2 3,24				**22**	

	Probability	**Impact**
Chief AM Architect	14%	66%
Blockchain Expert	26%	46%
Computing Infrastructure Expert	31%	77%
Chief Blockchain Architect	0%	2%

CURRICULUM VITAE

Matthew L. Scott
Charleston, SC
4/10/2019

EDUCATION

Purdue University 2001-2005 West Lafayette, IN
Bachelor of Science in Computer Graphics - focus in Manufacturing Graphics
Minor: Art and Design

Purdue University 2017-2019 (Online) West Lafayette, IN
Master of Science in Engineering Technology

MITxPro May 5,2018 - July 4, 2018 (Online) Cambridge, MA
Certificate in Additive Manufacturing for Innovative Design and Production

EXPERIENCE OVERVIEW

The Boeing Company 2005-Current Seattle, WA; N. Charleston, SC
Application Analyst/Developer Level 4

• Fully designed and collaborated with the Boeing Fire department on a smoke detection mounting system – 3D printed for testing. Patent awarded;
• Co-designed and 3D printed a cubical wall mount design which Boeing approved for patent, currently patent pending;
• Developed a method for automatically moving Big Data for Non-Destructive Inspection output;
• Chosen to lead a cross-functional team in an engineering program called “Innovation Cell” for five months. There I designed and provided 3D printed solutions for Boeing mechanics to help them save costs and reduce injuries;
• Brought a team of developers and engineers together to invent a fastener sorting device using artificial intelligence to save maximum cost for fastener reclamation – $11 million to possibly capture for Charleston alone. Received a merit award;

• Redesigned CATIA lab machine security to comply with Boeing security requirements;
• Hand-picked to join a team of 26 technical experts (called IT Technical Leadership Institute) to attack complicated technical issues in the company – Project: Business cases for wearable technology and authentication methods. Worked the agile process to develop software for storing voice recognition files and comparing to stored data on the exchange servers;
• Lead a project plan with BSC Engineering Integration to distribute and manage 3D printers across the site;
• Worked directly with BR&T (Boeing Research & Technology) scientists on additive manufacturing and non-destructive inspection projects;
• Organized and developed an enterprise website for additive manufacturing asset visibility;
• Developed a server/client utility (called SmartRDP) to aid CATIA experts when deciding what lab machine to log in to. Lean+ 10x development saved technical experts 1-2 hrs/wk in researching which machine has the software configuration they need for proper testing and if a machine was already logged in to;
• Developed and headed processes for test tracking, end user support, and mass server data collection;
• Continuously improving communication of information through visualization via webpages, charts, and diagrams for cross-function consumption;
• Leveraged existing tools to develop a program showing, via webpage, user logon utilization on Boeing South Carolina's HP BLADE workstations. This aided the end users (for machine brokering) and management (for utilization stats to help in purchase decisions);
• Engage in Lean+ endeavors by developing and automating work flow programs and processes;
• Adapted server-side expertise to support interns at Boeing South Carolina as their local Database Administrator and System Administrator for Windows 8 development;
• Managed server deployment and upgrades to DELMIA Process Engineer (the manufacturing process design and management tool for the 787 program);
• Trained in pertinent Lean and Agile business processes related to software deployment found within large enterprises;
• Combined knowledge in ENOVIA (engineering lifecycle management) with DELMIA Process Engineer to coordinate CATIA (engineering design) products and DELMIA processes while teaming in the enterprise;

• Aided and trained end users of the DELMIA and CATIA application through support and communications;
• Established an unprecedented relationship with ENOVIA IT to provide change management functionality linking the two systems together for the manufacturing change process via webservice technology;

Garrity Tool Company 1997 - 2005 Indianapolis, IN
Machine Operator
• Assisted machinists as a machine operator for the production of consumer and sensitive military products on CNC machinery;
• Inspected precision machined parts for high quality controls utilizing GD&T specifications;
• Gained understanding of G and M-Code for NC programming;
• Organized and managed shipping and inventory processes;

The Exponent 2004-2005 West Lafayette, IN
Graphic Artist
• Designed instructional graphics for news articles
• Created pictorial views to describe the writer's story
• Developed new layouts to incorporated graphics for standard news print

APPLICATIONS / PROGRAMMING SKILLS

• Expert in CATIA, DELMIA, ENOVIA (Product Lifecycle Engineering and Manufacturing)
• Expert in Adobe Photoshop, and GIMP (2D raster graphics)
• Expert in Adobe Illustrator, and Inkscape (2D vector graphics)
• Expert in Microsoft Batch programming
• Expert in VISIO (advanced data connections)
• Proficient in Oracle SQL and PL/SQL development
• Proficient in Adobe Flash
• Proficient in MS SQL Server
• Proficient in 3DS Max, Maya, Rhino, Blender, Sketchup (3D Modeling)
• Proficient in HTML, CSS
• Novice in VBA for Excel, Outlook, Word
• Novice in VB Script, VB, C#, C++, Python, Unix/Linux