SANS Institute
Information Security Reading Room

When a picture is worth a thousand products: Image protection in a digital age

Shawna Turner

Copyright SANS Institute 2020. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

When a picture is worth a thousand products: Image protection in a digital age

GIAC (GLEG) Gold Certification

Author: Shawna Turner, shayananna@gmail.com
Advisor: Sally Vandeven
Accepted: September 2nd, 2017

Template Version September 2014

Abstract

Today, a lack of fashion industry specific information security controls and legal protection puts fashion industry companies at significant risk of Intellectual Property theft and counterfeiting. This risk is only growing as traditional methods of manufacturing are rapidly evolving toward digital models of design and mass production, using Industrial Control System (ICS) approaches for mass production. As mass production moves to digital manufacturing, the effect of losing new product 2D and 3D imagery, as well as the speed and lack of traceability around those losses could significantly impact corporate bottom lines and risk profiles.

© 2017 The SANS Institute Author retains full rights.

1. Introduction

Today, a lack of fashion industry specific information security controls and legal protection puts companies that generate consumer products at significant risk of Intellectual Property theft and counterfeiting through image loss. This risk is only growing as traditional methods of manufacturing are rapidly evolving toward digital models of design and creation, which can use Industrial Control System (ICS) approaches for mass production (Luczkow, 2016). As mass production moves to digital manufacturing, the effect of losing new product imagery, as well as the speed and lack of traceability around those losses will significantly impact corporate bottom lines and risk profiles.

Historically, computerized automated manufacturing was limited to the production of items that are always the same. Each manufacturing machine was capable of producing a single part in a single size. The efficiencies came from the ability to create a production line that then assembled all the respective parts into a physical product, such as a plane, which is why this was called hard goods construction. Unlike airplanes, fashion has multiple sizes in production at any given time and usually has at least four seasons of unique product per year. The various size and rapid product changes involved with fashion made this older model of manufacturing less attractive or cost efficient. With the evolution of newer manufacturing capabilities and improved computer aided design tools, this is changing. Innovations in complete garment knit machines and 3D printing, driven by computer aided design (CAD) tools optimized for broad user adoption provide the opportunity for fashion to join other industries who receive efficiencies from computer automated manufacturing.

Companies that generate consumer fashion products create a variety of imagery associated with the design, approval and creation process of that product. In this case, 'fashion product' is being defined as any item purchased by a consumer in a store (virtual or physical) and may be apparel, footwear or equipment (accessories). The 2D images or 3D CAD models associated with product creation and distribution have monetary and brand value. That value can be positively or negatively impacted based on when and how

© 2017 The SANS Institute Author retains full rights.

consumers access that design, as well as how accurate and representational of the final product the imagery is.

The type of product picture produced has a direct relationship to the impact of image theft or loss to the company. A line art image of the product is worth less than a picture. The higher the volume of pictorial images and the more detailed and photorealistic the images are, the more value that collection accrues. In the case of either a line art image or a photorealistic 2D image, a competitor company or counterfeiter must still reverse engineer the product to make a competitive item. That costs both time and money before the competition can begin accruing benefit from the creative organizations' investment. Historically, the time it takes to reverse engineer a product and then scale for mass production often allowed the original design company to recoup the cost of the initial innovation.

Traditionally, designers only generated line art and photographic 2D style content for most of the life cycle of a product. Now, more and more of the design and mass production of fashion items are digitized, enabling not just more rapid innovation and product creation, but faster counterfeiting and intellectual property theft. If the imagery obtained was a 3D printer CAD drawing, then a competitor company (or counterfeiter) can make something that is effectively binarily identical using minimal to zero reverse engineering dollars and time. Additionally, the counterfeiter can start creating competitive products as soon as they can send the bytes to the right type of manufacturing equipment - which could be from minutes to just seconds later (Mendis, 2014).

The rapid turnaround of identical competitive product(s) means that the original brand that invested in the research and development to make a new, potentially cutting edge product(s), will lose much, or even all, of the market and brand advantage of that effort. At the very least, the company that was the creative source will have a significantly shortened lead time to get some return value out of the product investment before the competition can undercut them in the open market.

The cyber security product space has seen a proliferation of new product capabilities that have had a positive effect in most industries at reducing the attack

© 2017 The SANS Institute Author retains full rights.

surface. The reason the risk of image loss remains significant to companies operating in the fashion manufacturing industry is that neither security controls, or legal precedent, offer fashion-specific support. The concept of traditionally defined defense in depth provides necessary, but insufficient protection for image based intellectual property. While other industries, such as automotive and movies also contain images that are of significant business value, this paper focuses on the fashion industry, which does not receive equal legal protection. The security controls for images are industry agnostic. Consequently, the security controls suggested in this paper are not limited to just the fashion industry.

2. Current Protections

2.1. Legal Review

2.1.1. Copyright

In the US, laws about Intellectual Property referenced by visual images do not provide clear guidance about the representative image of a corporately owned product (such as a picture of a new sports shoe, material or technology.) For example, copyright protects the particular creative aspects of the visual image but not the subject or underlying event of the photo (Ekstrand & Silver, 2014). Protected content under the Copyright Act includes pictorial, graphic, and sculptural works — "two-dimensional and three-dimensional works of fine, graphic, and applied art."

Not all product creation efforts are considered equal. While it seems fashion design (including items like shoes, apparel, etc.) should qualify under the Copyright Act, garments are excluded by the "useful article" doctrine, based on their utilitarian function. For illustration, a shoe is meant to cover the foot, and all the decoration on, or technology in, the shoe does not change the function of footwear - to protect the foot. The law finds clothes utilitarian (Mendis, 2014.) "How do you separate the design of an item of clothing from the role of that item?"

2.1.2. Trademark

Trademark does not specifically address the technology advances in the fashion area either. Trademark law protects brand names, logos, symbols (think the LV for Louis

© 2017 The SANS Institute Author retains full rights.

Vuitton), designs and other optional elements of apparel and accessories - not the design itself. Trade Dress law does protect the appearance of an item, but the item has to be so distinctive that customers recognize it as being associated with the brand. The Supreme Court has held that "design, like color, is not inherently distinctive" for protection by trade dress because the purpose of design is considered only to be to make the item more useful, not indicate who created it. Traditionally, trade dress protects the design, packaging or appearance of apparel and accessories - but only to the level that the design identifies the source/origin of the product(s). To illustrate this, consider that a pair of jeans contains protectable elements - a vendor can register the brand name and logo hang tag with distinctive pocket stitching as protectable trademarks. However, that does not protect the actual design and technology of that pair of jeans, including color, materials, seam technology (such as welding vs. sewing), silhouette, etc.

2.1.3. Patents/Design Patents

The last available branch of protection in the US is patent law. Design patents in the US function similarly to registered designs in other countries, and are the only section of the patent law that applies to fashion. The US design patent protects the ornamental design elements for an object having practical utility. According to Forbes, a design patent provides 14 years of exclusive industrial design rights for new and non-obvious ornamental designs of functional items (Herzfeld, 2013). The question at the heart of design patentability is whether the presentation or appearance of the functional item is unique. It focuses on protecting the look, not the functionality.

A design patent was the basis of a jury verdict for Apple in the case of Apple v. Samsung. That outcome, where Apple won, spurred a number of fashion companies to add new US design patents, in addition to pre-existing Intellectual Property (IP), for protected designs ("More Designers Add Design Patents to the Mix But What About Trade Dress?" 2017). Design patents are a useful protection element, but the limitation to the look of a functional element means that a design patent does not protect new materials, methods of manufacture, or any other non-visible component.

Legal protections are typically considered the option of last resort. In cyber security, the traditional mantra is Prevent, Detect, Respond. Only after all of those steps

© 2017 The SANS Institute Author retains full rights.

have been taken, and property loss has occurred, do organizations seek redress through the courts. Risk-based spending would indicate the companies should start by focusing on identifying the best possible security controls for images.

2.2. Enterprise Security Image Controls

2.2.1. Digital Rights Management (DRM)

The primary loss prevention methods the cyber security industry offers for images are focused on providing attribution, not preventing image loss (Pesce, 2008). The standard for this is currently watermarking, which is considered a subset of Data Rights Management (DRM.) A subsequent section will cover watermarking.

DRM is fundamentally rights management, focused on enforcing end user content permissions to digital content (Lu, 2016). Today, DRM offerings are proprietary, which creates challenges working across multiple organizations or environments. For instance, in the fashion industry, designers work for a brand and get approval for a 2D or 3D image of the desired product. Once that image is approved, a new phase of work begins to validate the representation can become a mass produced tangible product. This process is known as commercialization. For commercialization, most fashion brands send selected images to a contracted manufacturing company. The manufacturing company takes the graphic content from the brand and recreates some percentage of them into a digital format that interoperates with the manufacturing systems they use.

Since the product image left the network and systems of the design shop, if a proprietary DRM product is in use at the design house, that DRM must be removed from the representations before sending them to the factory. The need to remove a proprietary product leaves the intellectual property unprotected by DRM as it changes hands. Because DRM is not interoperable and licenses are per company in the chain, the only way for the design house to make sure the factory applies DRM is by contract enforcement.

Additionally, the file formats supported by DRM tools out of the box do not reflect the standard design software used by people that work in the creative fields, such as artists, designers, etc. DRM tools are currently optimized to protect Microsoft Office and PDF content, not 2D design software, such as Adobe Illustrator, or 3D modeling

© 2017 The SANS Institute Author retains full rights.

software, such as CAD. Additionally, digital manufacturing equipment often has proprietary software associated with it. Because digital manufacturing is a new model for fashion, DRM vendors have not yet prioritized either 3D or proprietary digital manufacturing formats for interoperability.

In some cases, the current limitations of supported file formats are likely due to public perceptions around what rights anyone should have to images (Luo & Mortimer, 2016). For example, in 2015, the JPEG committee discussed adding the ability to add DRM to the JPEG standard. The Electronic Frontier Foundation (EFF), traditionally associated with protecting your rights online, provided a presentation arguing that enabling DRM in JPEG images 'would not be effective at protecting intellectual property rights in images and would have unwanted side effects.' Specifically, the concerns were that DRM does not handle copyright limitations well, such as fair use, and could be used for region coding, or even infringe on freedom of expression (Malcolm, 2015). Concerns about copyright limitations will probably continue to limit the available scope of DRM relative to some common file formats.

Regardless of particular file format issues, the EFF presentation does not suggest remediation for the economic value of protected images or the ability to protect intellectual property rights. To remedy the challenges with intellectual property rights, the EFF proposed cryptography, watermarking and steganography. These options center around the idea that intellectual property related to images is about attribution of the photo source. For fashion companies, attribution is only part of the concern. Additional concerns that weren't addressed by the EFF presentation include managed distribution, non-repudiation, and protection of company confidential imagery. Managed distribution is the ability to share files with other businesses, like manufacturing partners, without removing existing DRM security controls, for any supported file format.

DRM as a system makes certain environmental assumptions that impact the ability to provide managed distribution of images. The first assumption is that only finished products (images, videos, etc.) need DRM. By only protecting finished items, DRM does not protect against the insider threat, or accidents of disclosure that can occur during the design or initial production stages in the fashion industry. A side effect of this

© 2017 The SANS Institute Author retains full rights.

assumption is that creation tools do not natively contain DRM. Creation is when the intellectual property value of imagery starts.

For internal access to digital rights management, enterprises purchase DRM as a separate, completely stand-alone utility. Consequently, to properly integrate DRM into a fashion design workflow requires additional process and systems to be inserted, and leaves digital assets that have not been run through a DRM system unprotected. Ideally, DRM should evolve to be like application logging has become, where any intellectual property protection capabilities are native and have a default minimum level incorporated in the design applications used in the enterprise. Taken further, just as application logging functions, DRM should have a variety of pre-defined protection settings that allow for remote management of access rights by default.

This forward looking vision of DRM relies on the idea of a full format specific interoperability approach. Full interoperability would mean that an enterprise can apply DRM to a supported file type, and any authorized business partner could see the content of that file without needing the source company to remove the DRM. Today, full interoperability does not yet exist in the DRM industry, although research exists around what is required to achieve this capability (Lu, 2016). Once this capability exists, it will have broader applications than the fashion industry. For example, this capability would potentially reduce the number of leaks of pre-release movies and TV shows, such as exposure of Game of Thrones season 7.

2.2.2. Data Loss Prevention (DLP)

Data Loss Protection (DLP) solutions typically either use patterns of known attacks (signature–based) or try to find deviations from normal behavior (anomaly-based). Anomaly-based solutions can find unknown attacks. However, they typically have a high false positive rate, limiting their applicability to the detection of suspicious activities. Signature-based solutions can identify known attacks, which means they cannot recognize unknown attacks, or unusual paths (Constante, Fauri, Etalle, Hartog & Zannone, 2016). Signature-based solutions rely on fingerprinting. When a set of data has a hash value generated for it, that hash value is known as a fingerprint. Fingerprinting

© 2017 The SANS Institute Author retains full rights.

confidential documents or database records (e.g., credit card number) is very effective for organizations that primarily operate in Office suite applications to prevent data loss.

There are also DLP methods that create a model of sensitive values using keywords, regular expressions, text classification, and information retrieval, to detect the presence of confidential data leaving the organization perimeter. As images do not center around words, for DLP, they are considered unstructured data. Fingerprinting an image is therefore considered performing unstructured data fingerprinting, and there is a known performance penalty that increases as the number of fingerprints increase (Wittkop, 2016). Keywords or phrases do not apply to image property. Notably, there is no orientation to video or 2D/3D images, both of which are the primary and proprietary information for media and fashion organizations.

The fashion industry creates intellectual property primarily through the use of images. Each article of fashion will have a set of images associated with the item. For example, a pair of shoes likely has a sketch image, a photorealistic ¾ view, a picture of the sole; and a top down view of the shoe. This proliferation of images means that for performance reasons it is not practical to create an unstructured data fingerprint for every image that is created by the organization. Additionally, the type of 3D design image that could run a manufacturing system is a new area in the market, which means there is no DLP support for protecting that category of imagery.

2.2.3. Watermarking

DLP software often contains the capability of Digital Watermarking. Digital Watermarking is the practice of embedding extra information within digital content, also called host data, without interfering with the normal usage of data. Since the late 1990s, there has been an explosion in the number of Digital Watermarking techniques developed mostly for the rights protection of multimedia content (Panah, Van Schyndel, Sellis, & Bertino, 2016). For non-multimedia purposes, the security of watermarking is less well understood and defined.

Watermarks are about adding additional information to a file. A fingerprint is a watermark that is different for each item or instance and can uniquely identify the legal recipient of an authorized copy. Consequently, the source of improperly or illegally (re-)

© 2017 The SANS Institute Author retains full rights.

distributed content can be traced. One of the most referenced applications of digital watermarking is proof of ownership in a court of law, in particular when multiple ownership claims exist. By itself, while excellent for attribution, Digital Watermarking does not directly enable the traditional security orientations of prevention, detection, and response.

2.3. Enterprise Security Standard Controls and Images

2.3.1. Endpoint

Traditionally, endpoint protection referred to signature based anti-virus software. In recent years, the corporate environment has undergone significant change, which has changed the tools applied to the endpoint. More employees work remotely, often accessing contents resident in public, private and hybrid cloud environments. Corporate endpoints spend more time off the company network and have been joined by bring-your-own-device (BYOD) smartphones, tablets, and laptops, increasing the attack surface. The expanded attack surface led to a new type of security product called endpoint detection and response (EDR). EDR places agents on the endpoints to analyze application activity, sending information to a server in the cloud where their behavior is categorized, enabling the system to detect and flag anomalous activity (Kellett, 2016).

Signature-based antimalware, or next generation endpoint protection (NGEP), can detect known attacks while the cloud based anomaly detection and machine learning aspects of EDR primarily focus on prevention of new attacks against the file types considered typical. EDR and NGEP support the standard file types generated by Microsoft Office as well as PDF. Today these tools do not protect 2D and 3D file types. Given the 2D moving to 3D image orientation of the fashion industry, which will make it more profitable to exploit, there is likely more risk of zero days, or previously unknown attacks, coming in this space.

2.3.2. Network

Traffic volumes are increasing, and end-user usage patterns and needs are rapidly evolving, which impacts the traditional network (WAN, LAN, and mobile) designs. As companies adopt mobile and cloud, the perimeter is becoming increasingly difficult to enforce and protect. Several philosophies and technologies have been developed to meet

© 2017 The SANS Institute Author retains full rights.

these new demands, including software defined networking (SDN), cloud computing, and network function virtualization. These approaches focus on decoupling network capabilities from proprietary data centers with hardware appliances and providing network controls by the use of programmable software (Liyange, Ahmad, Okwuibe, Yilanttila, Sandots & de Oca, 2017).

The networking paradigm is converging towards software based and defined networking. In SDN, like many things, its primary strengths are also weaknesses. A driving reason behind the need to evolve traditional networks was data and application sprawl. By centralizing network control, SDN lets companies resize network needs and capabilities on the fly to respond to the continually expanding universe of data and applications. The application management side has not kept up with the network side for managing the threat landscape. This lack of application management can create situations where the team faces either restricting business ability by blocking unknown applications, in favor of security, or taking on risk related to a lack of app and data controls to enable business. As an industry, fashion trends toward having a high-risk appetite, in part because innovation drives a fail fast mentality that can extend to partnerships, tools, applications, etc.

Additional feature and vulnerabilities exist. SDN separates the control plane to centralize permissions and capabilities. That centralized control area means that operational malfunctioning or malicious software can compromise the whole network by getting access to that control plane. In general, the switch to software to manage all network configuration and capacity management provides a rapid response ability. That agility comes with the inherent weaknesses of software, particularly API enabled platforms. Defects are a fact of life when developing software, and can be leveraged to perform malicious activities, at any level the network touches.

Another feature of SDN is that traditional perimeter defenses, such as firewalls are now software deployable. These features can be used to track the ingress and egress of files through the network. In an environment like fashion, with its high-risk orientation, the primary use for the network as security ends up as the response function. When a design hits the streets early, or a competitor suddenly leaps several years closer

© 2017 The SANS Institute Author retains full rights.

in a new technology race, the incident responders will utilize the information logged and contained by these devices. The ability to understand what happened makes quality network capabilities important but does not help provide prevention and detection ability (Liyange et al., 2017).

2.3.3. Logging

Applications and network infrastructure components provide logs which then get aggregated in a single tool, traditionally a security information and event management (SIEM) system. SIEM software collects information and combines that data with other information about the users, assets, threats as well as other perceived vulnerabilities and correlates them. The goal is for the SIEM to perform real-time security monitoring and historical analysis (Liyange et al., 2017).

Some recurring challenges in SIEM limit the real world capabilities of the tool in a large enterprise environment. In the case of large environments, the analysis of logs for multiple appliances and their correlation is difficult. Performance penalties exist, and those penalties increase as the volume of data to be correlated increases. To address this requires a significant investment in skilled people and architecture. Regardless of organizational size, deploying and managing a SIEM solution is expensive and needs dedicated and experienced people. There is a scarcity of that skillset, which can result in a less than fully baked SIEM deployment, leading to a false sense of security (Alam, Ihsan, Khan, Javaid, Khan, Manzoor …& Farooq, 2016).

2.3.4. IT Security Best Practices

Many organizations use well-known IT standards, such as the ISO 27000x series, Control Objectives for Information and Related Technologies (COBIT), and related frameworks to protect themselves against security incidents. However, these standards, while well publicized, are very complicated and expensive due to the need for both trained people and technology resources to implement. Unfortunately, due to the complexity, cost, and extensiveness of these frameworks, corporations rarely reach a fully implemented standard. This issue of complexity may cause the enterprise to fall back to ad-hoc implementations of specific focus areas and quick-wins.

© 2017 The SANS Institute Author retains full rights.

Organizational characteristics influence the measurement of capability maturity within an organization. These can be internal factors, such as how many employees are part of the enterprise and what amount of revenue gets generated, as well as external factors, such as what sector the organization operates in or the geographic location of a firm. Funding and risk appetite should be used to gauge the target capability maturity of an organization. Regularly reviewing both key factors can help IT information security stay aligned to the goals and desired security maturity of the business.

The best practices build on each previously established layer of control, creating a circle of increasing virtue as more controls are applied. Cyber security best practice recommendations have an initial emphasis on compliance and policy. Without compliance and policy, companies cannot formally prove their security responsibility. Compliance also covers external requirements that other organizations impose, such as federal, partner, or international guidelines. User related aspects, such as awareness training, are the second area of focus. User awareness training is to drive a robust security culture and employee set of behaviors, when working internally or with external partners or vendors.

Once tone from the top and user training are checked off, organizations then focus on operational aspects of security. To identify what remediation is required, analysis of information risks and business continuity plans occurs. Physical security and adequate maintenance of IT infrastructure must be provided then monitored for violation and remediation. A competent security management team undertakes all of the identified security related work including the evolution of the organization's security maturity model.

Progress against the work is measured using key performance indicators aligned to business objectives and published broadly. Ongoing feedback cycles enable more strategic implementations of security that focus on what is truly important. Knowing the goals allows for better security trade offs based on maturity, capability, and funding targets.

Author Name, email@address

© 2017 The SANS Institute Author retains full rights.

2.4. Industrial Control Systems

2.4.1. Background

Industrial Controls Systems (ICS) is a general term that covers several types of control systems. An ICS consists of combined control systems that work together to achieve an industrial objective, such as manufacturing (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015). Traditionally, ICS are assumed to primarily apply to utility industries, such as electrical, oil, water, gas, etc.

With the evolution of mass production to a digital model, this is a less charted use of ICS security control approaches. With mass production manufacturing, specifically, fashion manufacturing, moving to digital models of design and production it is needful to identify which ICS security recommendations, in addition to traditional enterprise controls, apply to this evolution of mass production. The combination of legal coverage, combined with technical control review, should enable information security practitioners who work with images to better identify risk and remediation associated with image protection.

ICS control the physical world, and IT systems manage data. ICS have many characteristics that differ from traditional IT systems, including different risks and priorities. ICS use operating systems and applications that may be considered unconventional in a typical IT network environment. ICS operating systems and control networks are typically very different from IT counterparts, requiring different skill sets, experience, and levels of expertise. Assumptions that differences are not significant can have unfortunate consequences on system operations.

2.4.2. Industrial Control Challenges

The ICS space brings unique challenges. Many ICS processes run continuously and depend on the output of previous stages for inputs. Each phase also uses ICS systems, setting up a cascade effect where each stage has a defined input and expected output which drives the next stage. In other words, traditional ICS relies on interconnected and serialized steps of product construction. Consequently, if one phase breaks, the cascade effect could completely halt all production at the facility.

© 2017 The SANS Institute Author retains full rights.

For systems that control industrial processes, unexpected outages are not acceptable. Expected outages often must be planned and scheduled days or weeks in advance, with exhaustive pre-deployment testing to ensure compatibility both in the target stage, and every stage of production there after. Control systems often cannot be easily stopped and started without affecting production. Typical IT strategies, such as rebooting a component, are usually not acceptable solutions because of the negative impact a reboot would have on the requirements for high availability, reliability, and maintainability of the ICS.

Additionally, ICS and their OSs are often resource-constrained, and possibly real-time, systems that do not include typical contemporary IT security capabilities. Legacy systems lack resources common on modern IT systems (such as encryption, error logging, password protection, etc.) The expected life cycle of the hardware exacerbates the risks associated with this difference. Typical IT components have a lifetime of 3-5 years. For ICS where technology was, in many cases, designed for very specific use and implementation, the life of the ICS technology is often expected to be closer to 10-15 years and sometimes longer.

The operational and risk differences between ICS and IT systems create the need for increased sophistication in applying cyber security strategies (Stouffer et al. 2015). The cyber security industry has not yet embraced the idea that Industrial Control Systems may be endpoints. A particular example is in the domain of forensics. IT forensics has historically focused on the idea of turning off or suspending systems to protect evidence. The money making capabilities of manufacturing reside on those systems being perpetually online. The uptime requirements create a dilemma where a responder must decide whether to isolate a compromised system, leaving the application processes in a potentially unsafe state, or continue to operate, knowing that ongoing operations could overwrite valuable evidence. Additionally, most forensics tools and processes are designed to support Internet Protocol (IP) systems. However, ICS systems driven by Programmable Logic Controllers (PLC) have historically operated using different, and often proprietary protocols.

Author Name, email@address

© 2017 The SANS Institute Author retains full rights.

Fashion is always changing, based on consumer preferences. This quick evolution requires fashion providers to change at least as rapidly as consumer taste to maintain market share. Likewise, fashion oriented ICS, such as 3D printing for mass production, is undergoing significant, rapid evolution to mature the space (Shipp, Gupta, Lal, Scott, Weber, Finnin,... & Thomas, 2012). In combination, this has implications for the change management aspects of managing a fashion ICS. Industrial control systems will need to be regularly updated, which will require a streamlined onboarding and offboarding process. The rapidly evolving systems are unlikely to reside on a manufacturing floor long enough for many traditional ICS compensating controls, like policy masks or rigid change control, to be an effective approach.

A rigorous change control strategy needs a significant investment in time. For mass production, it is desirable to maintain continuous product manufacturing. The 24x7 nature of mass production makes a strict and detailed change control program improbable for a comparatively high system turnover environment. This issue of quick ICS machine evolution resulting in system turnover applies to all traditional IT and ICS security controls capable of being applied. As the fashion ICS market evolves, and ICS security and process controls grow with it, the ability to have more defined and rigid security policies, procedures and change management will increase.

2.4.3. ICS Security Best Practices

The ICS information security manager should identify which existing practices to leverage and which practices are unique to the control system. Build and train a cross-functional team that can share their varied domain knowledge (such as IT staff, control system engineers and operators, and enterprise risk.) There should be an ICS oriented information security program, which includes existing IT information security practices and ICS specific practices. Implement an ICS security risk management framework, and perform a risk assessment. Implement the security controls that mitigate the assessed risks. ICS networking and identity management will need particular attention.

When designing a network architecture for an ICS deployment, it is usually recommended to separate the ICS network from the corporate network, using both segmentation and segregation. Traditionally, Internet access, FTP, and email should not

© 2017 The SANS Institute Author retains full rights.

be allowed on the ICS network. The fashion industry does not traditionally perform mass production; factory partners do this. To get the right final product often requires multiple iterations on the design. To support several revisions, some amount of remote access, or preferably, a dual homed file share, may be beneficial to support transferring fashion designs between the fashion vendor and the factory partner, such as recommended by NIST 800-82 (Stouffer et al., 2015). To enable information transfer from the corporate network to the ICS networks may require additional configuration of some of the boundary protection devices, such as a stateful firewall. If the corporate facing file share resides in a DMZ, then no direct communication path would exist between the enterprise network and the ICS network, significantly reducing the risk.

Boundary protection can be used to protect the ICS by enforcing specific security policies. Gateways, routers, firewalls, guards, network based malicious code analysis and virtualization systems, intrusion detection systems (networked and host-based), encrypted tunnels, etc. are considered boundary protection controls. These devices determine whether the particular data transfer is permitted, usually by examining the data or associated metadata. Many traditional network architectures exist that leverage these controls to fit the fashion enterprise's need and budget. Some ICS oriented modifications to traditional network architectures are detailed out in NIST 800-82, Guide to Industrial Control Systems (ICS) Security.

Beyond network architecture and design, a defense-in-depth design provides additional risk mitigation. The architecture should include the network design, as well as effective security policies, training programs, incident response mechanisms, physical security, identity management, monitoring, logging, and where applicable for the ICS devices, local system controls, such as anti-malware. Each of these capabilities should be layered to provide maximum protection.

Identity management considerations interact with network design. For ease of administration, a centralized identity management capability, such as Active Directory or LDAP, is traditional for IT environments. ICS systems frequently utilize proprietary identification mechanisms that by default do not interface with third party servers and protocols, for example, LDAP. ICS systems with proprietary identity tools need manual

© 2017 The SANS Institute Author retains full rights.

updates with additions and changes to user permissions, complicating identity management. With the current rapid evolution occurring in fashion oriented ICS, specific care may be required to manage this risk. Having accountable resources in the ICS facility can address this both with specific on and off boarding process, as well as regularly scheduled manual true-ups from the central identity repository to the identified ICS proprietary identity managed systems.

A fashion oriented ICS will likely be a combination of a few legacy systems with planned long life spans (such as digital material cutters), and newer ICS that are undergoing significant rapid evolution, such as 3D printers. Because of this hybrid environment, it may be difficult or infeasible to apply some of the traditional security controls, such as those defined in NIST SP 800-53. In many cases, the underlying theme of the control is still applicable. For example, Role Based Access Control (RBAC), which is common in traditional IT environments, often doesn't have interfaces to the authorization mechanisms of ICS equipment. To enable RBAC would require the development of a specialized interface software if the ICS can work with a centralized identity store or a custom implementation of RBAC if the ICS system has a proprietary identity management mechanism.

Also, ICS systems are not designed to the same standards as IT systems and may have password sizes and rotation requirements very different from IT standards used to provide RBAC. Coupled with the likelihood of ICS systems having proprietary identity management mechanisms, and the high probability of insecure network protocols if passwords are transmitted, a key risk reduction strategy is to have separate password policies and standards for the ICS environment from the IT environment. The use of multiple password policies and standards would mitigate risks where the corporate IT policies could be detrimental to the operation of the ICS system. Password management and rotation can be supplemented or modified by the use of rigorous physical security controls, either to the ICS space, or the individual ICS systems.

Similar to password challenges, patching brings unique concerns in ICS environments. Some ICS systems utilize older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable.

© 2017 The SANS Institute Author retains full rights.

Other ICS systems use operating systems that do not receive regular patching. With the high requirements around uptime, as well as patch acquisition and management challenges, the burden of testing, including regression testing increases. Some ICS systems require that the vendor of the ICS system create custom versions of patches for the base operating system for compatibility reasons. Outage windows between IT and ICS systems are unlikely to align. With this list of concerns, consider separating the patch process between the two environments, IT and ICS.

Fashion as an industry implements ICS in ways that are very unlike critical infrastructure, or traditional hard goods mass production. When manufacturing a hard good, something like a plane, an individual system will always have the same order of events and size of thing to generate. In fashion, the order of events and size of an item will be variable. A shoe has to come in a run of sizes from a smaller size to a larger size. Shoes could involve actual sewing of components, heat welding, layering of elements, etc.

Historically, to change the size of an item being produced by ICS required a significant effort in building custom programming for the system. To run the size modified program required a non-trivial process of loading and unloading the custom size program as appropriate. This level of effort meant that most systems were not set up to perform dynamic size changes, and switches to create new size runs were carefully planned and scheduled to minimize impact to production thruput. The variability required for the fashion industry creates challenges for traditional ICS security approaches.

In a traditional ICS security model, if a car part significantly varies from baseline in production, it is probably an introduced defect. That presumed error could be used to generate an alert, which could indicate a possible corruption or security issue on the system. When the product runs are variable, changes to size, color, etc. can not be used for alerting. Today, for fashion ICS, reviewing the outcome most production runs cannot be fully automated and requires human intervention. Over time, new models of comparing manufacturing result to baseline will need to be evolved, enabling identification of security issues that occur in variable sized manufacturing ICS, like fashion.

Author Name, email@address

© 2017 The SANS Institute Author retains full rights.

As the fashion industry is new to the use of ICS for mass production, they are less represented in organizations focused on sharing information related to ICS. The ICS-CERT is a fundamental component of the DHS Strategy for Securing Control Systems. The ICS-CERT coordinates control systems related security incidents and information sharing with Federal, State, and local agencies and organizations. Fashion organizations should pursue active involvement with ICS-CERT. Over time, fashion can provide visibility and lessons learned into the communal CERT environments. These experiences should help both existing companies that use commercial security tools, as well as the next industry to adopt the evolving capability of digital design through mass production.

3. Conclusion

The evolution of fashion makes for a fascinating space involving overlap between law, traditional Information Technology, and Industrial Control Systems. Current frameworks do not fully support the unique uses cases associated with fashion mass production. For each of these spaces (law, IT, ICS), challenges exist that lead to future opportunity.

The use of law for fashion will continue to be a court of last resort to protect intellectual property. Efforts to address the gaps that would allow the law to be used more proactively for fashion continue. As fashion, law, and technology continue to increase in overlap, there will continue to be the desire to clarify what protections are available through what legal means. Technology companies have already begun using existing fashion oriented protection, like Design Patents, and have the knowledge, opportunity, and resources to help shape future legal conversations that impact fashion. Evolving technology law could provide significant momentum for fashion law change in the future.

The second area of focus, IT controls, has traditionally focused on corporate owned systems in the context of an enterprise. Existing best practices still provide a security foundation to protect Intellectual Property residing on corporate computers. Initiatives to tightly integrate mass production to digital design capabilities creates new opportunities for IT controls to expand beyond the corporate network. In the future, these IT capabilities may span multiple companies as well as reach into spaces traditionally

© 2017 The SANS Institute Author retains full rights.

considered purely ICS. Hopefully, future intellectual protection capabilities in IT technologies, for example, DLP, DRM, and watermarking, will expand to support that future overlapping IT and ICS landscape.

Lastly, the use of ICS in fashion is a relatively new development, which is still evolving. In traditional ICS, such as car manufacturing, designing and implementing a new system, or automated capability is very rare. (Stouffer et al. 2015). Many existing best practice security approaches for ICS rely on this low turnover for compensating controls. The security technologies and methodologies have the opportunity to evolve in parallel with the changing models of manufacturing.

Customer fashions change rapidly. Fashion ICS is a developing area, and new systems and software are quite common as an industry evolves. Regular changes to systems create new risks. Those risks will need regular reviews and alignment with existing security IT and ICS implementations, evolving business risk appetite, and current funding model.

Fashion manufacturing will continue to strive to be efficient, data driven, adaptive, and flexible to stay aligned to consumers. The end goal of bringing fashion to automated manufacturing is to provide individualized, but mass-produced product to buyers. The customizable product will need a user interface for consumers, as well as a secure way to send the customer designs to the production facility for rapid creation and distribution. The user interface components will be manageable using traditional IT and IT information security capabilities. The ability to protect the design in transit to the factory has some support via traditional IT controls, like encryption, but true defense in depth protection could come from the ability of traditional corporate IT image protection controls to be more extensible into new environments, like factory partner and ICS networks.

In addition to user interface and design transport capabilities, production facilities will need to evolve to support individualized mass production. Manufacturing plants will involve more information and communication technology, as well as new connections traversing multiple systems, production facilities, and the cloud. Traditional information security and manufacturing did not encompass these expectations, so the existing

© 2017 The SANS Institute Author retains full rights.

information security controls are not (yet) prepared for this environment (Haverkort & Zimmerman, 2017). True defense in depth security is achievable as ICS, and IT technologies expand to support this new model of manufacturing. This evolution of protecting the imaged based intellectual property has business value based on the assumption that other mass production oriented industries will adopt this integrated approach of rapid development.

Market leaders take advantage of unexpected opportunities. Mass produced personalized fashion seems likely to count as an significant opportunity for both security personnel and security tools vendors. While a unique market, the mass produced fashion security concerns echoes themes common across security in both IT and ICS spaces. Future security capabilities for all industries are experiencing a push toward portability, both across systems and networks. For example, many security concerns related to the Internet of Things (IoT) are very similar to themes identified for fashion mass production. The potential for a new advancement in security controls supporting both IoT, and fashion ICS offer a significant chance for vendor differentiation and infosec tools capability expansion to occur. Hopefully, this deep dive into the fashion mass production provides interesting security insights into a market not traditionally studied for security or ICS.

Author Name, email@address

© 2017 The SANS Institute Author retains full rights.

4. References

Alam, M., Ihsan, A., Khan, M. A., Javaid, Q., Khan, A., Manzoor, J., ... & Farooq, S. (2016). Optimizing SIEM Throughput on the Cloud Using Parallelization. *PloS one*, *11*(11), e0162746.

Costante, E., Fauri, D., Etalle, S., Den Hartog, J., & Zannone, N. (2016, May). A hybrid framework for data loss prevention and detection. In *Security and Privacy Workshops (SPW), 2016 IEEE* (pp. 324-333). IEEE.

Devlin, R. (2015). *Data Loss Prevention*. Retrieved from https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-37152

Ekstrand, V. S., & Silver, D. (2014). *Remixing, Reposting, and Reblogging: Digital Media, Theories of the Image, and Copyright Law.* Visual Communication Quarterly, 21(2), 96-105. doi:10.1080/15551393.2014.928155

Haverkort, B. R., & Zimmermann, A. (2017). Smart Industry: How ICT Will Change the Game!. *IEEE Internet Computing*, *21*(1), 8-10.

Herzfeld, O. (2013). *Protecting Fashion Designs*. Retrieved from Forbes website: https://www.forbes.com/sites/oliverherzfeld/2013/01/03/protecting-fashion-designs/#3438d4b3b317

Johnson, C. W. (2016). Why We Cannot (Yet) Ensure the Cybersecurity of Safety-Critical Systems.

Kellett, A. (2016). 2017 Trends to Watch: Security.

Kundur, D., Lin, C. Y., Macq, B., & Yu, H. H. (2004). Special issue on enabling security technologies for digital rights management. *Proceedings of the IEEE*, *92*(6), 879-882.

Liyanage, M., Ahmad, I., Okwuibe, J., Ylianttila, M., Kabir, H., Santos, J. L., ... & de Oca, E. M. (2017). Enhancing Security of Software Defined Mobile Networks. *IEEE Access*.

Lu, W. (2016). Effective Rights Exporting Process-Towards system interoperability of digital rights management.

Author Name, email@address

© 2017 The SANS Institute Author retains full rights.

Luczkow, A. M. (2016). *Haute off the Press: Refashioning Copyright Law To Protect American Fashion Designs from the Economic Threat of 3D Printing*. Minnesota Law Review, 100(3), 1131-1170.

Luo, H., & Mortimer, J. H. (2016). *Copyright Infringement in the Market for Digital Images.* American Economic Review, 106(5), 140-145. doi:http://dx.doi.org/10.1257/aer.106.5.140

Malcolm, J. (2015). *Copyright, Code and Creativity A Note of Caution About DRM in JPEG*. Retrieved from Electronic Frontier Foundation website: https://www.eff.org/files/2015/10/13/jpeg_presentation.pdf

Mendis, D. (2014*). 'Clone Wars' Episode II—The Next Generation: The Copyright Implications Relating to 3D Printing and Computer-Aided Design (CAD) Files*. Law, Innovation & Technology, 6(2), 265-281.

Milano, D. (2012). Content control: Digital watermarking and fingerprinting. *White Paper, Rhozet, a business unit of Harmonic Inc., http://www. rhozet. com/whitepapers/Fingerprinting—Watermarking. pdf, Last accessed May*, *30*.

More Designers Add Design Patents to the Mix But What About Trade Dress? — The Fashion Law. (2017). Retrieved from The Fashion Law website: http://www.thefashionlaw.com/home/more-designers-add-design-patents-to-the-mix-but-what-about-trade-dress

Panah, A. S., Van Schyndel, R., Sellis, T., & Bertino, E. (2016). On the properties of non-media digital watermarking: a review of state of the art techniques. *IEEE Access*, *4*, 2670-2704.

Pesce, L. (2008). *Document Metadata, the Silent Killer...* Retrieved from https://www.sans.org/reading-room/whitepapers/privacy/document-metadata-the-silent-killer--32974

Shipp, S. S., Gupta, N., Lal, B., Scott, J. A., Weber, C. L., Finnin, M. S., ... & Thomas, S. (2012). *Emerging global trends in advanced manufacturing* (No. IDA-P-4603). INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA.

Stouffer, K. A., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015). Guide to industrial control systems (ICS) security. *Special Publication (NIST SP)-800-82 Rev 2*.

Author Name, email@address

© 2017 The SANS Institute Author retains full rights.

Wittkop, J. (2016, November 4). Best Practices for Tagging and Protecting Documents with Data Loss Prevention. Retrieved September 1, 2017, from https://www.linkedin.com/pulse/best-practices-tagging-protecting-documents-data-loss-wittkop-cissp

Author Name, email@address

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Last Updated: August 15th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS FOR508 Sydney August 2020	Sydney, AU	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Virginia Beach 2020	Virginia Beach, VAUS	Aug 30, 2020 - Sep 04, 2020	Live Event
SANS London September 2020	London, GB	Sep 07, 2020 - Sep 12, 2020	Live Event
SANS Baltimore Fall 2020	Baltimore, MDUS	Sep 08, 2020 - Sep 13, 2020	Live Event
SANS Munich September 2020	Munich, DE	Sep 14, 2020 - Sep 19, 2020	Live Event
SANS Australia Spring 2020	, AU	Sep 21, 2020 - Oct 03, 2020	Live Event
SANS San Antonio Fall 2020	San Antonio, TXUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS Northern VA - Reston Fall 2020	Reston, VAUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS FOR500 Milan 2020 (In Italian)	Milan, IT	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Amsterdam October 2020	Amsterdam, NL	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Brussels October 2020	Brussels, BE	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Prague October 2020	Prague, CZ	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS London October 2020	London, GB	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS Orlando 2020	Orlando, FLUS	Oct 12, 2020 - Oct 17, 2020	Live Event
SANS October Singapore 2020	Singapore, SG	Oct 12, 2020 - Oct 24, 2020	Live Event
SANS Stockholm October 2020	Stockholm, SE	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Dallas Fall 2020	Dallas, TXUS	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Rome October 2020	Rome, IT	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS SEC504 Rennes 2020 (In French)	Rennes, FR	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Cologne October 2020	Cologne, DE	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS San Francisco Fall 2020	San Francisco, CAUS	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS Geneva October 2020	Geneva, CH	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS SEC560 Lille 2020 (In French)	Lille, FR	Oct 26, 2020 - Oct 31, 2020	Live Event
SANS Tel Aviv November 2020	Tel Aviv, IL	Nov 01, 2020 - Nov 05, 2020	Live Event
SANS London November 2020	London, GB	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Rocky Mountain Fall 2020	Denver, COUS	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS DFIRCON 2020	Miami, FLUS	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Sydney 2020	Sydney, AU	Nov 02, 2020 - Nov 14, 2020	Live Event
SANS Krakow November 2020	Krakow, PL	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Paris November 2020	Paris, FR	Nov 02, 2020 - Nov 07, 2020	Live Event
APAC ICS Summit & Training 2020	Singapore, SG	Nov 13, 2020 - Nov 21, 2020	Live Event
SANS OnDemand	OnlineUS	Anytime	Self Paced
SANS SelfStudy	Books & MP3s OnlyUS	Anytime	Self Paced