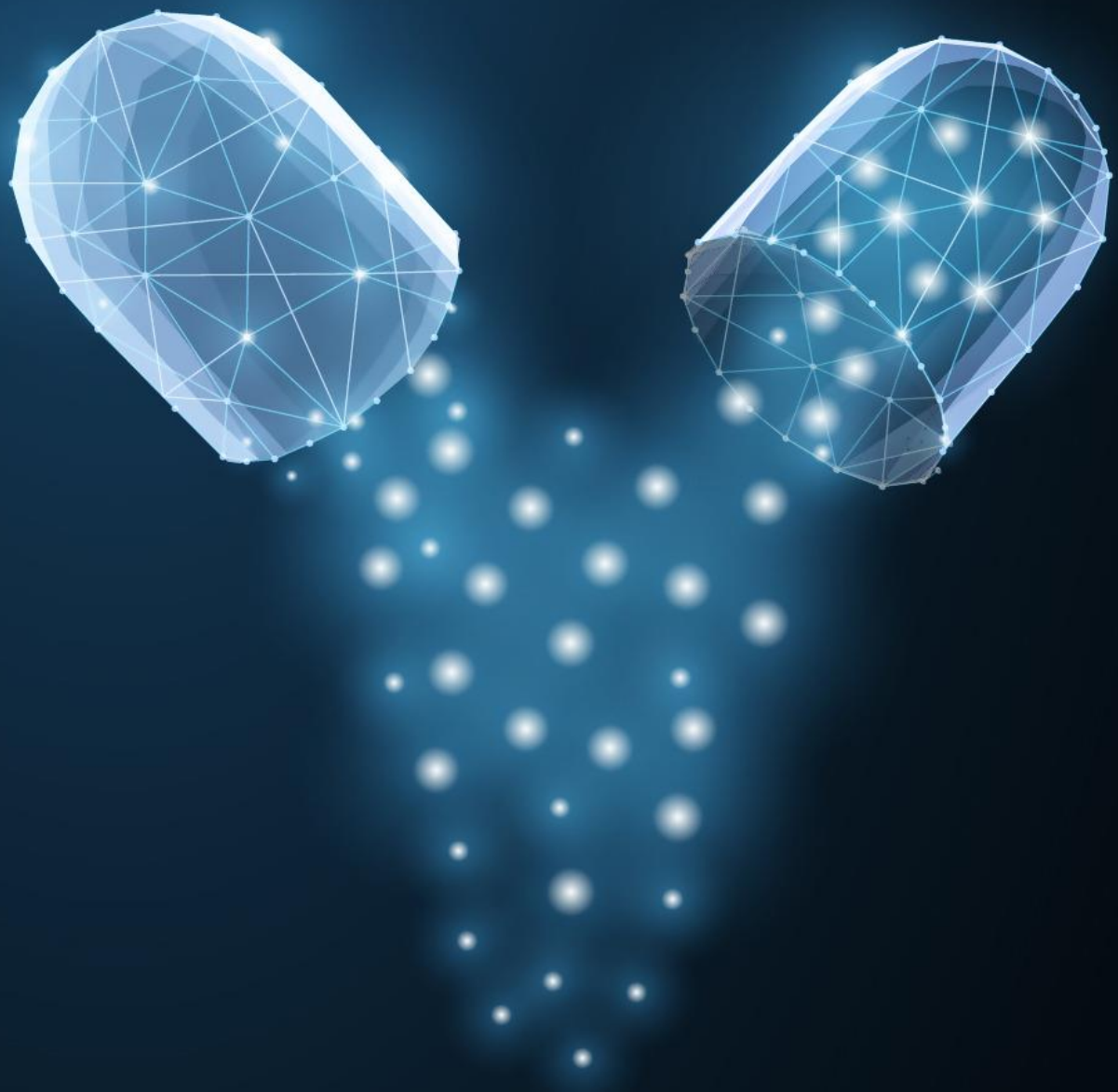


# HEALTH INDUSTRY CYBERSECURITY
# PROTECTION OF INNOVATION CAPITAL

**MAY 2020**

Healthcare & Public Health Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

## Disclaimer

This document is provided for informational purposes only. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all healthcare organizations, nor is it intended to be an exhaustive or definitive source on safeguarding intellectual property, trade secrets or other forms of innovation capital.

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

# About

### The Healthcare and Public Health Sector Coordinating Council Joint Cybersecurity Working Group

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector, critical healthcare infrastructure entities organized under Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Joint Cybersecurity Working Group (JCWG) is a standing working group of the HSCC, composed of more than 200 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Recommendations for the Protection of Innovation Capital is the product of Task Group 1C5, established under the auspices of the HSCC JCWG and composed of medical technology, health IT, as well as HHS, to address a major recommendation of the Healthcare Industry Cybersecurity Task Force report from June 2017 calling for a cross-sector strategy to develop such recommendations.

To provide feedback on this tool, please send comments to **Feedback@HealthSectorCouncil.org**.

For more information on the HSCC, see **https://HealthSectorCouncil.org**.

# Members of the Working Group

The following individuals constitute the membership of the committee established in April, 2018, who were responsible for development of the observations and recommendations on Intellectual Property Protection.

**Task Group Co-Chair, Greg Barnes**, Chief Information Security Officer, Amgen
**Task Group Co-Chair, Russell Koste**, Chief Information Security Officer, Alexion
**Terry Rice**, Health Sector Coordinating Council Chair, Chief Information Security Officer, Merck
**Greg Garcia**, Executive Director, Health Sector Coordinating Council
**Omar Tisza**, Business Operations Coordinator, Health Sector Coordinating Council
**Mike Towers**, Chief Security Officer, Takeda
**Ryan Schreck**, Associate Specialist IT Risk Management, Merck
**Michael E Hale**, Senior Security Engineer, Cedars Sinai
**Tom Chmielarski**, Director of Information Security & Data Protection, Abbvie
**Mark Schildkraut**, Associate General Counsel, Beckton Dickinson
**Nathaniel McInnis**, Associate Director, Abbvie
**Scott Bourne**, Senior Specialist IT Risk Management, Merck

### Advisors

**Upasana Tripathi,** Director, PricewaterhouseCoopers (PwC)
**Joe Shepley**, Managing Director, Ankura
**Kevin Rosenbaum,** Of Counsel, Mitchell Silberberg & Knupp LLP and Counsel to the International Intellectual Property Alliance (IIPA)

### Special Thanks To

**John Trudeau**, Trudeau Creative
**PricewaterhouseCoopers (PwC)**
**Greg Garcia,** Executive Director, Health Sector Coordinating Council
**Samantha Jacques,** McLaren Health, for the constructive feedback
**Marian Merritt**, Lead for Industry Engagement, National Initiative for Cybersecurity Education (NICE) - National Institute for Standards and Technology (NIST), for the comprehensive, and exceptional editing advice



## Signature Page

(Intentionally Blank)

# Table of Contents

**Table of Figures**

# Executive Summary

This paper intends to serve as a resource to security and risk practitioners at any stage of their information protection program's maturity, with a particular focus on Innovation Capital (IC) protection. It also gives senior management and boards of directors a framework for discussions with security and legal practitioners on the risks to shareholder value and how it's being defended. Be it program start-up, or maturation of an established function, the information provided here encompasses emerging trends, best practices and lessons learned from mature teams across the healthcare industry.

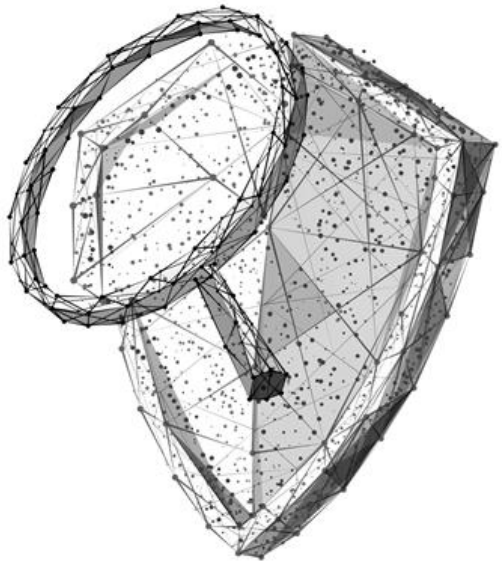
This paper highlights the important differences between protecting IC versus other categories of sensitive corporate data (e.g., protected health information, payment card industry, personally identifiable information).The findings and recommendations in this document are focused at helping practitioners effectively protect corporate IC without duplicating general cybersecurity frameworks or recommendations available elsewhere. We assume familiarity with core cybersecurity approaches and modalities (e.g., identity and access management, end-point protection, and classification) only insofar as they need to be adapted to meet the distinctive requirements of IC protection. Within, we extract lessons and themes from notable instances of IC theft, devoting special attention to emblematic case studies. We provide the reader with a broad understanding of U.S. and international legal remediation trends, outline enforcement challenges, and share a range of specific information protection control recommendations to improve healthcare IC protection overall. Case studies highlight factors that enable IC theft, factors leading to the detection and defense against IC theft, and the significant business consequences resulting from each loss.

Following the illustrative case studies, this document sets forth various recommendations on controls for protecting IC, ranging from proactive governance and legal safeguards, to protective controls, to monitoring and response to address theft. These controls are discussed in depth and should be considered in both the context of the case studies as well as the environment of the reader.

Throughout, the reader will find control examples and recommendations generally grouped into one of two categories: Passive or Active Measures. Whereas Passive Measures largely refers to non-automated, non-preventive controls, as well as administrative elements such as governance and oversight, policies and procedures, awareness and training, and audit, Active Measures largely refers to and involves the use of extant technologies, detective and preventative controls, applications, and practices for automated, continuous and real-time (or nearly real-time) information asset identification, disposition for protection, lifecycle management and data control.

# Introduction

The loss of IC would be expected to adversely impact an organization's ability to develop or maintain global market position,



develop revenue, or, in the worst cases, fund future innovation.

The term IC, as it is used in this document, refers to non-public intellectual property, trade secrets, business models, data sets and derived insights, process controls, methods for using types of data, and the like.

To ensure the recommendations in this document result in the strongest form of protection of IC, it is just as important to understand what IC *is not*. Personal Identifiable Information (PII) for example, is not IC, and therefore it, and Privacy as a general matter, is outside the scope of this paper. Data or insights from data regarding business operations that are not expected to uniquely yield capital or cost avoidance outcomes are not IC; neither are publicly accessible scholarly papers or articles and output which inform idea generation engines. This is not to say these things are not worthy of protection, only that broadly speaking, they are outside the scope of the definition contemplated here.

It is disappointing, particularly in the United States, that the interests and concerns of private industry, law enforcement, and the nation continue to deeply complicate our collective ability to aggressively enhance Innovation Capital (IC) protection. Even as the need to appropriately protect active investigations disinclines law enforcement agencies from sharing timely, specific observed threat information with the rest of the industry, little to nothing is being done to assist future victims in the analysis of the risk to themselves, or to learn the observable behaviors, tactics, campaigns and trends in IC theft, loss, and exposure which might threaten them.

This lack of information sharing, particularly without swift, proportional and responsive penalties, arguably incentivizes adversaries to continue a divide and conquer strategy against corporations, both nationally and across the globe. Similarly, victims fail to share information regarding active or closed incidents involving IC theft with industry peers, shareholders, or the public, potentially out of a desire to avoid negative publicity, frivolous or ill-conceived lawsuits,

or perceptions of negligence. This combination of factors is *actively* contributing to an erosion of the value of the national interest; protection of the world's foremost innovation economy.

Although recommendations like those contemplated in the 2019 Intellectual Property (IP) Commission on the Theft of American Intellectual Property (IP Commission) Review, where the Securities and Exchange Commission would examine whether companies' use of stolen IP should be publicly reported to strengthen accountability requirements for firms seeking a listing on U.S. exchanges (IP Commission, 2019), could be a step in the right direction, none as of yet address the conflicting interests between law enforcement, private companies and national interests.

IC risks generally fall into five broad categories: loss, exposure, theft, assurance of integrity, and assurance of availability. Although we stipulate the latter two are also important for IC protection, they have more to do with business process continuity assurances (the likes of which modern ransomware frequently disrupts) and fall outside of the focus of this paper. Herein, for the purpose of obtaining a manageable set of recommendations, we generally focus on the first three categories, as they fall squarely in the zone of IC protection.

**IC carries at least seven distinct protection challenges:**

1. It represents a subset of the broader range of data that information protection professionals safeguard, which equally complicates the process of asset inventory and data protection.

2. The breadth of access to IC required to innovate can sometimes outpace the ability to control or protect the data from those who might abuse it.

3. Most organizations lack a sustainable process to identify and control their most valuable data.

4. Given the variety of technologies and use cases for access to and appropriate sharing of IC, suitable protective controls are either inordinately expensive or simply unclear.

5. Organizations apply data governance decisions inconsistently. While 'governance' attempts to solve for who has decision rights, outcomes suggest this is not keeping pace with industry's need for speed, transparency and multi-party access.

6. The shift towards adopting external and cross border digital collaborations, including software as a service (SaaS) and cloud hosted IC, and third-party

services partnerships[1] dramatically complicates discovery, management and protection of IC physically, technically, legally, and administratively.

7. Protecting citizen, patient/customer and employee privacy is now an organizational mandate for most institutions around the globe. Many reactionary privacy remediations can, unfortunately, complicate an organization's ability to actively monitor and protect IC.

Technology innovators devoted nearly half a century to enabling processing speed and the seamless movement of data across systems and organizations without always considering the security challenges posed by these new data processing and communication modalities. In the grand scheme of things, we are only recently shifting, placing economic value on secure processing and secure collaboration.

With the notable exception of U.S. Department of Defense classification standards[2], there are no laws, regulations, or industry standards which prescribe how organizations manage, mark, or designate sensitive information. In 2011, the SEC made a cautious first step at cybersecurity oversight of public companies traded in the U.S. marketplace. This guidance was again updated in 2018 to strengthen disclosure requirements for public companies experiencing material cybersecurity risks and incidents (Parrish, 2018). This is still a far cry from regulating the management of impactful information. Many would argue this might even be a good thing — at least until protection norms can be relied upon by corporate leadership and shareholders.

If a medical device manufacturer, for example, wishes to publish its designs freely on the internet or share them openly with partners and others, no one will stop them—quite the opposite: third parties will clamor to access these designs and leverage them to their own advantage. As opposed to a Personally Identifiable Information (PII) or Protected Health Information (PHI) breach, both of which bring regulatory fines and sanctions (HIPAA Journal, 2015) as well as potential PR fallout, the visible impacts for IC leakage typically entail loss of market share, revenue, stock valuation or sales (or some combination of all three) without regulatory or legal consequences, as long as the owners of the IC do not pursue a claim. However, a period of sustained compromise across any particular market (or a national economy) will have significant longer-term economic and social impacts. Invisibly eroding innovation engines, slowly, inexorably impeding the flow of innovative products to consumers through localized impacts, and ultimately suppressing vital nutrients to our national economy. If the focus of a targeted organization is in life

[1] For a comprehensive range of supply chain recommendations see **https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf**

[2] **https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001_vol2.pdf**

saving and life extending drugs or health products for example, the negative impacts of IC theft extend far beyond those companies; they extend into the health and quality of life for the communities they directly serve, national revenues, and taxes for the general welfare of the nation.

As information protection professionals, lawmakers, corporate boards of directors, and management turn to address how to protect this vital set of assets, the patchwork of existing regulations, laws, and standards (such as NIST, HiTECH, HIPAA, etc.) only take them so far; those protective efforts remain necessary but *insufficient.*

We set forth the following framework to actively protect organizational IC:

1. Continuous identification of IC
2. Assignment (and periodic update) of the estimated value and ownership of IC.
3. Establishment of comprehensive control and adherence/compliance requirements for IC.
4. Implementation of active and passive protective controls to close perceptible gaps (as outlined in the control recommendations).
5. Periodic, focused review and sustainment efforts

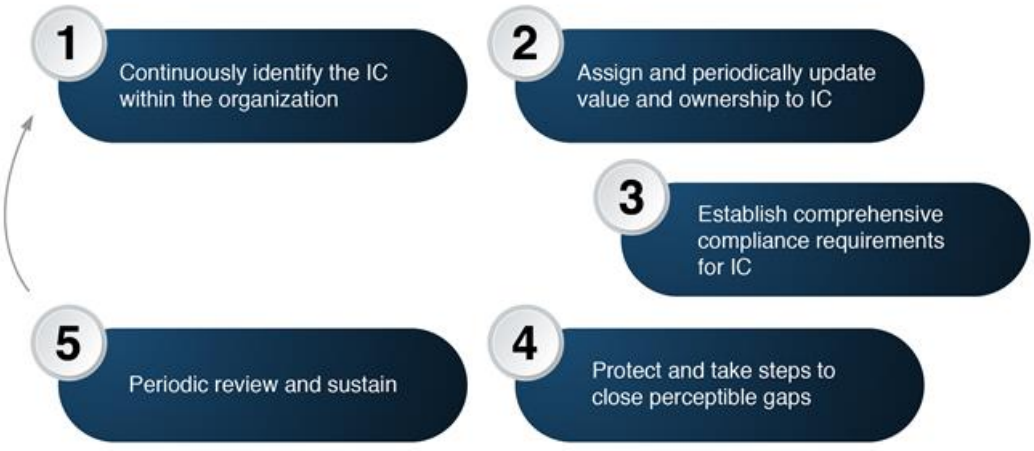



Figure 1. The IC Protection Framework

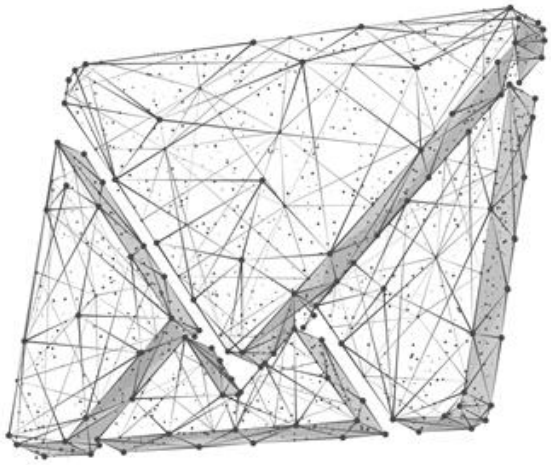
## IC Theft Case Studies

The theft of Innovation Capital is often not measured or broadly disclosed. Incidents that are disclosed via open litigation, prosecution, or media disclosure sometimes offer real-world learning opportunities to examine controls that were or were not applied, as well as how control gaps were exploited. But public examples of the theft of IC are rare. Victim organizations have little incentive to subject themselves to public scrutiny. Criminal and civil litigation, however, can be a useful source as they announce that an incident happened and describe relevant facts.

After reviewing numerous notable IC theft examples (listed in the **appendix**), we highlight several here for deeper analysis, in the form of case studies. These case studies depict the real-world impacts of IC theft and infringement ranging from individual-based insider threat to organizational and state sponsored theft among others. The incidents offer actual instances of significant business impact, and in this working group's opinion, exemplify the need for more effective public-private cooperation regarding IC protection.

**The following case studies and links to control recommendations are based on statements contained within the indictments and may not be a complete representation of the facts on control placement / effectiveness.**


### Case Study 1 - Conspiracy to Steal Pharmaceutical Trade Secrets



Several people conspired to steal trade secrets from the pharmaceutical company GSK to benefit a competitive company, Renopharma, that they founded (United States of America v. Xue, 2018). The conspirators included two scientists employed at GSK who subsequently pleaded guilty to stealing GSK trade secret information they had access to as part of their employment.

The indictment specifically noted that "GSK typically spent over $1 billion to research and develop each biopharmaceutical product" (U.S. Department of Justice, 2018). The multi-year collaborative theft of trade secrets benefited the newly founded

Renopharma by reducing the amount of investment, both financial and in effort, required for it to have marketable products. In particular, the indictment notes that the research and development of biopharmaceutical products poses "difficult challenges" in several ways and the stolen documents contained GSK trade secret and otherwise sensitive information on addressing those challenges (U.S. Department of Justice, 2018). In this way the GSK research directly assisted Renopharma by lowering Renopharma's go-to-market costs and timeframes.

**Relevant highlights from the indictment include:**

1. The collaborators founded a company, Renopharma, to capitalize on the stolen trade secret and confidential information for their own benefit.

2. The IC stolen was listed as a combination of GSK trade secrets regarding biopharmaceutical products under development as well as "research data, GSK's research and development processes, and GSK's manufacturing processes."

3. A collaborating/indicted GSK scientist "emailed GSK trade secret and otherwise confidential information relating to a dozen or more products and numerous GSK processes" from her work e-mail account to her personal e-mail account. This IC was then forwarded to other collaborators.

4. A collaborating/indicted GSK scientist "download[ed] a substantial amount of trade secret information from GSK's network onto a thumb drive or other portable storage device."

5. A collaborating/indicted GSK scientist stole information on GSK products in development, "even products she was not researching."

6. The indictment notes that the scientists had signed and/or been trained on numerous policies and agreements regarding the confidentiality expectations.

7. The allegation notes that a "substantial amount of trade secret information" was copied to a portable media device (U.S. Department of Justice, 2018)

8. Notably, GSK may not have adequately:

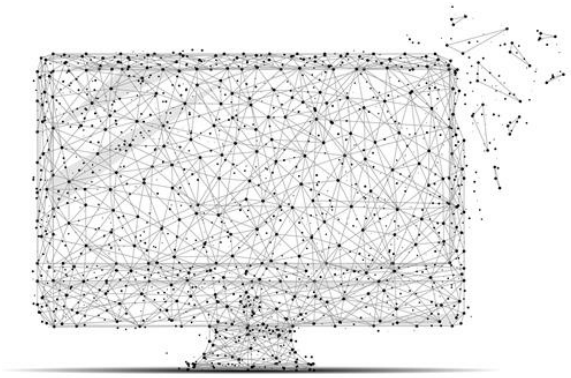
    a. Restricted access to data by employee role.

    b. Restricted download of sensitive company information to non-company storage devices.

    c. Blocked highly sensitive data from being forwarded from employee accounts to personal email addresses.

**d.** Restricted substantial downloads by company employees of company sensitive data.


## Case Study 2 - Theft of Development Medical Device Pen Injector



A former employee of a global medical technology company (Becton, Dickinson, and Company, "BD") attempted to steal IC for personal economic benefit (United States of America v. Maniar, 2013). The defendant was an engineer at the BD headquarters where he was a member of a group responsible for manufacturing pre-fillable syringes and pen injectors. In this capacity, per the indictment, he "had access to BD trade secret information related to the development of such products, including BD trade secret information related to a self-administered, disposable pen injector still under development and not yet released for commercial sale" (U.S. Department of Justice, 2013).

The indictment notes that it was critical to the success of BD that its research and development for future products remain secret and that the company took many steps to protect its trade secrets and confidential and proprietary information (U.S. Department of Justice, 2013). It also notes that BD's estimated costs associated with the disposable pen injector's development to be in the millions of dollars (U.S. Department of Justice, 2013).

This defendant worked at C.R. Bard, Inc. prior to his employment at BD, where he allegedly conducted IC theft in a similar fashion, with intent to combine the technologies from the two different companies to create wealth for himself. The focus of this case study only references the portions relevant to BD, but it's worth noting that more information regarding the allegations of his actions to harm C.R. Bard, Inc. can be found in the indictment itself which is listed under the reference material table.

**Relevant highlights from the indictment include:**

1. As early as October 2012 and while still employed at BD, the conspirator formulated a plan to start his own medical device manufacturing company in his home country (India).

2. While still employed by BD, and despite the fact that all employees had signed and/or been trained on policies and agreements regarding the confidentiality

of company information ("Employee Agreement", "Trade Secret Policy" etc.) and agreed to protect BD's trade secrets, the conspirator downloaded and exfiltrated approximately 8,000 files belonging to BD, using multiple computer storage devices. These files contained BD Trade Secret Information related to the disposable pen, including external hard drives and thumb drives.

3. The conspirator used his BD email account to forward the stolen documents containing BD trade secret information and confidential information relating to the disposable pen injector to his personal email account.

4. On or about May 23, 2013, the conspirator called in sick and did not report to work. This was also the day before his resignation. Instead, the defendant downloaded BD files using his mobile work laptop (U.S. Department of Justice, 2013).

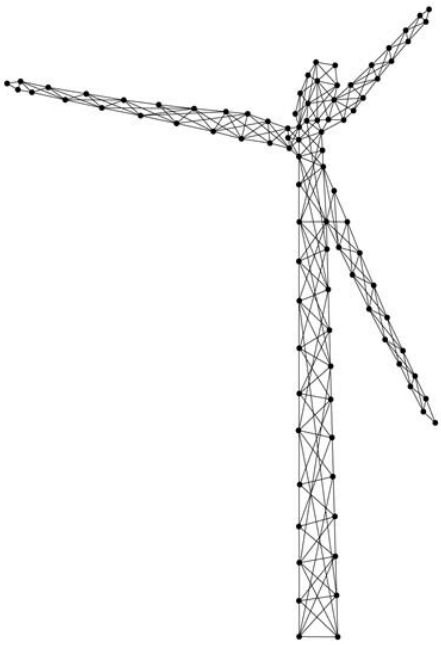
5. Notably, while BD carried a strong complement of passive measures, it may not have:

   a. Restricted download of sensitive company information to foreign storage devices.

   b. Blocked highly sensitive data from being forwarded from employee accounts to personal email addresses.

   c. Restricted unusually large downloads by company employees of company sensitive data.


## Case Study 3 - Wind Turbine Source Code Theft



The Sinovel Wind Group (Sinovel), a Chinese firm, was charged in June 2013 with trade secret theft. The firm's deputy director of research and development, along with a technology manager and an engineer, were all charged with stealing intellectual property information from AMSC, a U.S.-based company formerly known as American Superconductor Inc. Dejan Karabasevic stole the intellectual property from AMSC when he worked at the

company within the automation engineering department in Austria. Karabasevic was found guilty in Austria on related charges in 2011 (United States of America v. Sinovel Wind Group, 2013).
The indictment against Sinovel indicates that Karabasevic secretly downloaded, to aid Sinoval, source code on March 7, 2011, from an AMSC computer in Wisconsin to a computer in Klagenfurt, Austria. Sinovel then built several wind turbines in Massachusetts with AMSC's stolen software source code. The results of this industrial espionage were severe. AMSC lost more than $1 billion in shareholder equity and nearly 700 jobs, which represented more than 50 percent of its global workforce (U.S. Department of Justice, 2018). As a result, and after litigation, Sinovel was ordered to pay $1.5 million for the theft of AMSC, Inc.'s trade secrets. A few days earlier, Sinovel and AMSC agreed for Sinovel to pay $57.5 million in restitution (U.S. Department of Justice, 2018).

The two companies even had a partnership relationship that dated back to 2005. The companies worked on many large energy infrastructure projects. Sinovel provided the wind turbines, while AMSC provided the software code used in the turbines to control the flow of electricity onto the electrical grid. AMSC's software is provided for technology known as Low Voltage Ride Through (LVRT) (Getty, 2018).

**Relevant highlights from the indictment include:**

1. In March of 2011, Karabasevic submitted his resignation to AMSC, but still he retained access to the AMSC Windtec computer system into May 2011. His final day with AMSC Windtec was June 30, 2011.

2. The indictment reports that "it was part of the conspiracy that Sinovel, through [two Sinovel co-conspirators], recruited Karabasevic to leave AMSC Windtec and join Sinovel."

3. Between March of 2011 and June of 2011, Karabasevic clandestinely copied IC from the AMSC computer system, including the source code to one of AMSC's products.

4. In June of 2011, Sinovel offered Karabasevic a one-year employment contract. The contract "made it appear that Karabasevic would work for a Chinese wind turbine blade manufacturer from July 1, 2011, to June 30, 2012, in order to hide the fact that Karabasevic planned to work for Sinovel during the same period."

5. Sinovel then provided Karabasevic with a laptop with the intention to adjust AMSC's IC for Sinovel's unrestricted use. Karabasevic complied and provided Sinovel with AMSC proprietary software, technical information, and trade secret information.

6. This stolen innovation capital was then used by Sinovel to commission their own wind turbines in Massachusetts with software created from the stolen and modified AMSC source code (U.S. Department of Justice, 2013).

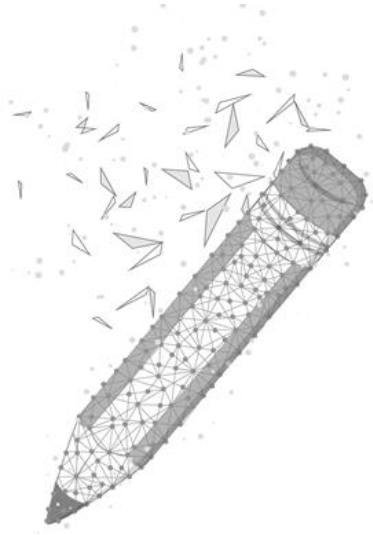
7. Notably, while the complainant carried a strong complement of passive measures, they did not appear to:

   a. Restrict download of sensitive company information to foreign storage devices.

   b. Block highly sensitive data (such as source code) from being copied to external, non-company systems.

   c. Restrict unusually large downloads by company employees of company sensitive data.


## Case Study 4 - Hacking of Academia by Iranian Mabna Institute



In 2018, nine Iranian nationals were indicted for conducting an enormous cyber innovation capitalIC theft campaign which heavily targeted academia on behalf of the Iranian Islamic Revolutionary Guard Corps (IRGC). In this campaign, the hackers "penetrated systems belonging to hundreds of universities, companies, and other victims to steal research, academic data, proprietary data, and intellectual property" (U.S. Department of Justice, 2018). The defendants sought out data from across numerous fields of research and academic disciplines, including science and technology, engineering, social sciences, medical, among other professional fields. The nine accused were all leaders, contractors, associates, hackers-for-hire,

and affiliates of the Mabna Institute, an Iranian company that was accountable for the operation of cyber invasions that began as early as 2013 into "computer systems belonging to 144 U.S.-based universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the United States Department of Labor, The Federal Energy Regulatory Commission, The State of Hawaii, The State of Indiana, The United Nations, and the United Nations Children's Fund" (U.S. Department of Justice, 2018).

The Mabna Institute targeted over 100,000 online accounts of professors around the world and was able to successfully compromise approximately 8,000 professor email accounts across the collective victims (U.S. Department of Justice, 2018). Through these activities, the Mabna Institute's intrusions yielded over 30 terabytes of academic data and IC from universities, and email inboxes from employees of victimized private sector companies, government victims, and non-government organizations (U.S. Department of Justice, 2018). This campaign was ostensibly executed on behalf of the Islamic Republic of Iran's (Iran) IRGC; one of several groups within the Iranian government responsible for gathering intelligence. This case was one of the largest state-sponsored hacking campaigns ever prosecuted by the Department of Justice. While it's difficult to quantify the value of the information stolen from the victims, it is estimated the U.S.-based universities spent approximately $3.4 billion to procure and access the data and innovation capital that was stolen through the course of this conspiracy (U.S. Department of Justice, 2018).

**Relevant highlights from the indictment include:**

1. The campaign was conducted across multiple stages. First, Mabna conducted online reconnaissance of university professors to evaluate their research interests and the academic articles that they published.

2. Second, using the information collected, the conspirators conducted email spear phishing to target selected professors. These emails were personalized and appeared to have been sent from a professor at another university.

3. If the targeted professor interacted with certain links in the email, they would be directed to "a malicious Internet domain named to appear confusingly similar to the authentic domain of the recipient professor's university."

4. When a professor entered his/her login credentials into the malicious links, those credentials were then logged and captured by the hackers for later use.

5. Finally, conspirators used the stolen account credentials to gain unauthorized access to their victim's accounts. Using victim accounts, they then "exfiltrated intellectual property, research, and other

academic data and documents from the systems of compromised universities, including, among other things, academic journals, theses, dissertations, and electronic books" (United States of America v. Rafatnejad, 2018).

6. While specific strengths and weaknesses associated with the protection of IC in this case are difficult to make, several high-level observations can be applied:

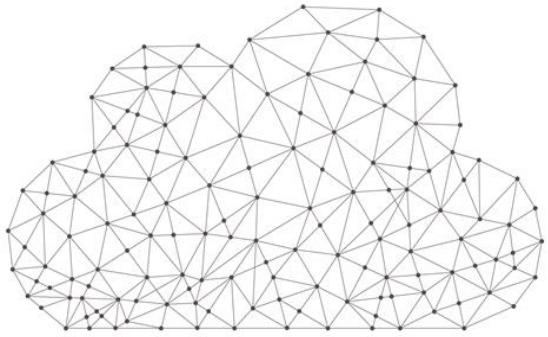
   a. Most of the email inboxes of the university professors were unprotected by multi-factor controls.

   b. Publicly exposed e-mail is a risky storage location for highly sensitive or valuable innovation capital. Separating communications methods from IC storage and access is one way to tackle this.

   c. Contextually sensitive login/Identity and Access Management policies could have provided early warning and/or restricted access to the victim mailboxes from unusual or foreign locations.

   d. A broad DMARC implementation will assist in the reduction of risk associated with intra and inter-university domain and account spoofing (for the purpose of phishing).


## Case Study 5 - "Cloud Hopper" IC Theft via Managed Service Provider Access



According to a December 2018 Federal Indictment, a Chinese-based Advanced Persistent Threat (APT) group compromised several Managed Service Providers (MSPs) to gain downstream access to the MSP customers and, ultimately, the IC within those customers (U.S. Department of Justice, 2018). This case highlights the security risks of corporate vendors and supply chain attacks. This attack group was given several names by their victims, and security researchers, with "APT10" being the most well-known. The multi-year campaign is often referred to as "Cloud Hopper".

As with Case Study 4, this example includes a threat actor who is a Nation State (China), meaning that the sophistication and resources behind the attackers will be more significant and defense will be that much more difficult. This attack campaign

impacted more than 45 companiesand occurred over a span of at least 12 years, indicating a deliberate long-term effort to steal IC (U.S. Department of Justice, 2018).

The indictment notes a strategy-shift for this long-term attack campaign, focusing on MSPs, in approximately 2014. MSPs often have administrative access to their clients, potentially with direct network access. While a company may have excellent security practices, safeguards, and monitoring it will still be very difficult for that company to determine that a system administrator from their MSP is stealing data from the systems they are administering. Additionally, targeting the MSP means that an attack group can compromise one company to gain access to dozens of target companies rather than compromising each of those individual companies directly.

The use of compromised system administrator accounts to conduct theft of IC will defeat many standard data protection controls, increasing the difficulty of defending against this attack vector.

**Examples include:**

1. Administrative tools normally (and should) use encryption, preventing network-based monitoring from identifying data movement (as with network DLP).

2. Administrators typically have significant, if not full, access to the data on the servers and databases they manage, so user-oriented access control and recertification will not help.

3. Administrators (or compromised administrators) are not likely to transmit data from DLP-protected end points.

4. IC governance, confidentiality agreements, and user awareness will not deter this type of theft.

In certain countries identified in the United States Trade Representatives Special 301 Report, particularly those with significant state owned enterprises (SOE), government-associated theft of IC can seamlessly feed back into company activities since the private/public distinction is minimal. According to the federal press release for the indictment, the targeted companies include “aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production” (U.S. Department of Justice, 2018).

**Relevant highlights from the indictment include:**

1. The hackers behind the attack worked for “a company in China called Huaying

Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau."

2. The theft includes (minimally) "hundreds of gigabytes of sensitive data" from the victim companies.

3. The transition to MSPs was "to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and steal, among other data, intellectual property and confidential business data on a global scale."

4. APT10 began its attacks with phishing, sending email with malware-infected document attachments, to target companies.

5. Once data was collected, the APT10 hackers "often used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before the final exfiltration" to APT10 systems (United States of America v. Hua, 2018).

The Cloud Hopper campaign used a variety of methods and attacks to gain access to the victims, move laterally within the victim companies and those companies' customers, and exfiltrate information. Controls that may have been lacking in the aggregated victims include inadequate:

1. Technical controls around email to detect and block phishing.

2. User awareness to detect and report phishing attacks.

3. Access monitoring to identify abnormal access to information (such as customer data files by an MSP system administrator).

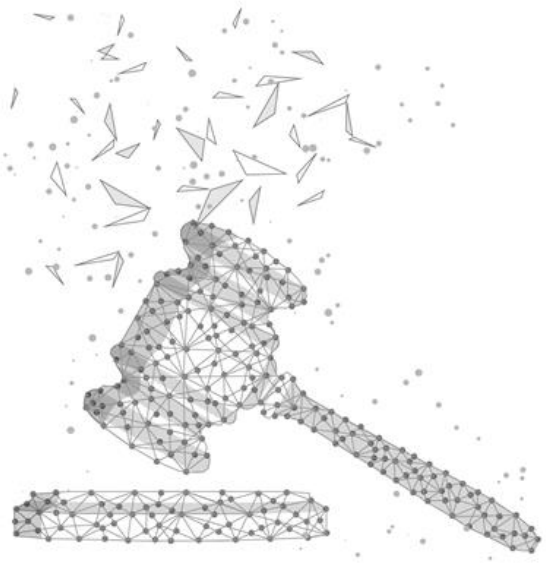
4. Multifactor authentication and privileged account management to limit the impact of compromised user accounts.

5. Data Loss Prevention technology to monitor unusual information movement (such as business records into an encrypted archive).

6. Network security technology to limit direct communication of IC laden servers to the internet.

# On the State of National and International Law

## Your Trade Secret Protection Program Sets a Foundation for Legal Safeguards



The purpose of this section is to outline the value of considering the current state of the law and its enforcement as it underpins certain trade secret protections within your organization's overall data protection program. Often the most valuable subset of an organization's innovation capital, trade secrets, are uniquely protected by the law. In the United States and Europe, when following processes to identify and protect trade secrets, organizations gain legal remedies if loss were to occur. Legislation in other parts of the world is also evolving, giving aggrieved parties stronger tools for possible recovery of information, damages and other forms of justice (such as deterrence arising from criminal prosecution). The data backs this up. Trends show ever more effectiveness in both civil and criminal courts, offering organizations both a deterrent and a remedy. If IC does leak from your organization, consider the possibility of pursuing a legal remedy rather than doing nothing.

Legal remedies are evolving, but generally are insufficient alone for aggressive protection of IC. Legal recourse generally falls into two categories: civil causes of actions (generally played out in court) and criminal causes of action involving law enforcement (e.g., Department of Justice, FBI).

Successful recovery of misappropriated intellectual property is always difficult and, at times, seemingly impossible to achieve. Notwithstanding advancements in legal systems in various jurisdictions as well as increased cybersecurity maturity and readiness by intellectual property owners, the incidence of successful protection and/or recovery of misappropriated intellectual property is growing.

Through the rest of this section, we provide clarity on the applicability, protections and remedies afforded to trade secrets.

### Trade Secrets

The principal body of legislation that protects intellectual property owners from

misappropriation of their sensitive and valuable information involves trade secret protection.

A subset of Innovation Capital, trade secrets are generally defined as information, regardless of its form (physical, electronic, etc.), as long as "(i) the owner has taken reasonable measures to keep such information secret; and (ii) the information derives independent economic value...from not being generally known to...another person who can obtain economic value from the disclosure or use of the information" (Legal Information Institute, 2019).

Examples of trade secrets might include, but are not limited to: methods that ensure high purity in pharmaceutical manufacturing, overall assembly-line mechanics, or specific chemical processing techniques that lower the cost of extracting compounds from supplies, scientific studies, chemical formulations, certain non-public financial information, sales and marketing strategies and computer programs.

1. **Secrecy**. In terms of secrecy, once the information is known — for example, by entering the public domain, permissible reverse engineering, or disclosure by the trade secret owner (whether purposeful or unintentional) — it will no longer be entitled to trade secret protection. (See, e.g., Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Article 39 (World Trade Organization, 2019).

2. **Reasonable Measures**. To qualify as a trade secret, the intellectual property owner must undertake "reasonable measures" to protect the information (18 U.S.C. § 1839(3)). This test focuses primarily on the actions of the owner and "depends on the extensiveness of the security measures and how well they are followed" (Toren, 2016). Under the Economic Espionage Act, the U.S. Congress intentionally did not define what constitutes a reasonable measure; rather, Congress stated "what constitutes reasonable measures in one particular field of knowledge or industry may vary significantly from what is reasonable in another field or industry and the owner of the information must assess the value of the material it seeks to protect, the extent of theft, and the ease of theft in determining how extensive their protective measures should be." Id. quoting (142 Cong. Rec. S12213 (daily ed. Oct. 2, 1996).

   Courts have defined reasonable measures to include advising employees of the existence of a trade secret, limiting access to the information on a need-to-know basis, requiring employees to sign confidentiality agreements, and keeping secret documents under lock. (Fenwick & West, LLP, 2001). Requiring employees, contractors, visitors and other people who may come into contact with trade secret information to sign confidentiality or non-disclosure agreements helps to ensure that the information retains its

trade secret protection, as such agreements impose on their signers a contractual duty not to disclose the information. Id.

3. **Economic Value.** Trade secrets must also inherently confer economic value by their secrecy. The intellectual property holder must show that their secrecy confers some sort of competitive, and often financial, advantage.

## Trade Secrets Law – U.S., European Union, and Beyond

If an intellectual property owner determines that its trade secrets have been misappropriated and is seeking remuneration in the form of recovery, cease and desist from using, damages and the like, the owner may have options through available legal systems for such recourse.

Companies involved in such a situation will generally attempt one or all of the following: recovery without the support of the legal system (e.g., no civil court system or law enforcement involvement);, commencing a civil action;, or making a criminal referral to law enforcement. Some question the effectiveness of trade secret law in addressing foreign espionage and nation-state backed IP theft. While its effectiveness is limited, organizations have successfully brought criminal indictments on actors operating within the United States (MAURIELLO, 2014).

1. **Recovery without Filing a Legal Claim.** In less complex matters — for example, where a former employee departs his or her company with limited amounts of trade secret material and has not made further dissemination or use; an intellectual property owner can seek recovery of its information, based on applicable law (trade secrets, employment law, contracts law), without resort to litigation or law enforcement means. This is often accomplished with a cease and desist letter or some other communication demanding the return of the misappropriated content.

   Additional measures that may be taken include: attaching a legal complaint, interviewing the former employee (to better understand the motive of his or her actions and confirm recovery), obtaining a signed declaration that all materials have been returned and not further used or disseminated, and

forensic inspection of the physical and/or electronic resources that contain or contained the misappropriated material. Due to the relatively low amount of resources (financial and human capital) associated with this form of recovery, this tends to be preferred when viable.

2. **Civil Action.** Fortunately, should an individual or company need to resort to the legal system, the trade secret misappropriation laws have been maturing and becoming more consistent — and thus more effective — particularly since 2016.

   a. **Defend Trade Secrets Act (DTSA).** Since May 2016, instead of or in addition to commencing a trade secret misappropriation action under state law, the U.S. has provided for federal civil protections for theft of trade secrets under the federal Defend Trade Secrets Act (DTSA). Since its enactment, the DTSA has been invoked in hundreds of cases (Brachmann, 2018).

      One powerful tool arising from the DTSA is the ability to seek an ex parte seizure. Such a seizure allows an intellectual property owner to go into federal court — without the accused's presence or knowledge — to effectuate an order to seize the misappropriated material from the premises or possession of the accused (18 U.S.C. § 1836(b)(2)). It is deemed an "extraordinary" measure and, as such, a plaintiff in such cases needs to meet certain requirements, such as a showing of irreparable harm, likelihood of success by the plaintiff, and that the defendant is in actual possession of the trade secret and/or property. *Id.*

   b. **EU Directive.** In 2016, the European Union issued a directive that aimed to standardize the national laws in EU countries against the unlawful acquisition, disclosure and use of trade secrets. EU countries were required to provide civil means through which victims of trade secret misappropriation can seek protection. (International Bar Association, 2018).

      The purpose of the EU directive is to address the significant variation of trade secret protection and enforcement across EU member states, some of which lacked significant protections. The European Commission's draft directive on the protection of trade secrets sought to provide a clear and uniform level of protection across the EU and to counteract the growing problem of trade secret theft (Winston & Strawn, 2019). It created a common definition of trade secret and set out the measures, procedures and remedies that member states should make available. (*Id*.) Another objective of

the EU directive is to facilitate cross-border research and development and allow more effective response to unlawful attacks on a company's know-how. *Id.*

c. **Other Jurisdictions.** The DTSA and EU directive have also sparked changes in other parts of the world. In recent months, for example, Japan amended its Unfair Competition Prevention Act and half of the 12 countries that negotiated the Trans-Pacific Partnership Agreement strengthened their trade secret provisions and enforcement regimes.

It is important to note that there is no international treaty specifically pertaining to the protection of trade secrets. However, the Trade-Related Aspects of Intellectual Property Rights (known as TRIPS) established by the World Trade Organization (WTO) establishes minimum standards for the protection of trade secrets (as well as patents copyrights, and trademarks) that each WTO signatory state must provide (World Trade Organization, 2019). Compliance with TRIPS is a prerequisite for WTO membership. *Id.*

3. **Other Cause of Action.** It is important to consider that other causes of action may be pursued. Some are specific to the U.S. and others are more broadly available.

For example, remedies may be available under the following laws (among others):

a. Computer Fraud and Abuse Act (U.S.): The law prohibits accessing a computer without authorization, or in excess of authorization.

b. Breach of Contract: Many employees sign an employee agreement, intellectual property assignment and/or confidentiality agreement that provides ownership and/or protection of company-related intellectual property (including trade secrets) accessed through working for the company. The obligations typically continue after employment ends.

c. Violation of Labor Law: Applicable labor laws bind a fiduciary duty of an employee to a present or former employer that prohibits theft of work product.

4. **Criminal Referral.**

a. **United States.** In 1996, Congress enacted the Economic Espionage Act (EEA). As reported by the Congressional Research Service (CRS), the legislative history of the EEA reveals the congressional concerns over growing international

and domestic economic espionage against U.S. businesses that prompted the establishment of a more comprehensive federal effort to protect trade secrets. (Unknown, 2014). The EEA sets forth two criminal offenses: theft of a trade secret for the benefit of a foreign entity (economic espionage, 18 U.S.C. Section 1831) and trade secret theft intended to confer an economic benefit to another party (theft of trade secrets, 18 U.S.C. Section 1832). To trigger an action under either provision of the EEA, the information must qualify as a trade secret as defined in the EEA. (Id.) While Section 1832 does not require that the offense benefit a foreign entity, the theft must economically benefit someone other than the trade secret owner. (Id.) Moreover, in Section 1831, the foreign economic espionage provision more broadly encompasses misappropriation for any purpose, including non-economic benefit. (Id.)

The EEA authorizes substantial criminal fines and imprisonment penalties for economic espionage and theft of trade secrets. For economic espionage, the maximum penalties reach $5 million for individuals and imprisonment of 15 years. Corporations found guilty of this offense are subject to a maximum fine the greater of $10 million or three times the value of the stolen trade secret. Theft of trade secrets for commercial advantage is punishable by a fine of up to $250,000 for individuals, as well as imprisonment of up to 10 years, whereas corporations can be fined up to $5 million. The EEA also authorizes the criminal or civil forfeiture of "any property used or intended to be used ... to commit or facilitate" an EEA violation as well as "any property constituting, or derived from, any proceeds obtained directly or indirectly as a result of" an EEA offense. Offenders must also pay restitution to victims of trade secret theft. Finally, during any prosecution or proceeding under the EEA, federal district courts are required to enter protective orders or to take other measures, "as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." (Id.)

**b. Europe.** While there are no criminal sanctions under the EU directive, EU countries are allowed to give more protections than under the EU directive. For example, under French criminal law, it is a criminal offense for a director or employee of a company to disclose a trade secret. It is therefore important to

understand the country-specific protections that are available in the jurisdictions that are relevant to an act of trade secret misappropriation.

## Practical Considerations

There are two significant decisions to consider when seeking to recover misappropriated trade secret materials. These are (a) which course(s) of action to pursue, and (b) which jurisdiction applies.

1. **Course of Action.** As set forth above, should trade secret misappropriation occur, the trade secret owner needs to determine whether to pursue recovery on its own, through civil action and/or criminal referral. Each measure comes with its own pros and cons. For example:

    a. **Recover on one's own**: This is less expensive but may not practically lead to recovery of the misappropriated information without having to file a civil claim or for law enforcement to open an investigation that can be put in place by a civil action or through law enforcement. (See below.)

    b. **Civil Action.** Civil action places more significant pressure on the accused, may enable seizure of property and restrictions on use and dissemination, and restrict travel. However, civil litigation can be costly in terms of outside legal counsel expenses and shifts company and employee focus away from day-to-day business dealings and toward legal matters.

    c. **Criminal Referral.** This enables maximum protections against the accused as such action could result in search warrant(s) to recover misappropriated materials and arrest warrant(s) to restrict ongoing wrongdoing. Criminal referral tends to cost less than to commence a civil action as the intellectual property owner (the victim) is not directly part of the legal action; rather the action is between the government and the accused. Giving control to the government could result in less control for the intellectual property owner; for example, the government may move at a pace that is unsuitable for the trade secret owner or decide to not act.

2. **Jurisdiction.**

    a. **U.S. State v. Federal Law.** It is important to consider factors that may dictate whether federal or state law provides the best available or more favorable remedies. Such factors include:

    "Whether the employer needs and qualifies for the protection of the civil ex parte seizure provision, a remedy

only available under the federal DTSA; and

"Whether the federal or state forum can best protect trade secrets during litigation.

b. **U.S./Europe Compared with Other Jurisdictions.** It is generally believed that the U.S. (and certain European countries) offer the most sophisticated and robust protection for trade secrets and that some other countries' laws respecting trade secret protection or enforcement are weak, and that "the issue is particularly acute in many of the largest emerging economies, such as China, Brazil, Russia and India." (Yeh, 2016)

Further, certain countries have been identified by the U.S. intelligence community as leading threat actors with respect to cybersecurity, e.g., Russia, China, Iran, and North Korea (Clapper, 2016). In addition, the U.S. government has identified the following countries as providing insufficient protection of intellectual property, and therefore remain on the Priority Watchlist of the USTR Special 301 Report: China, Indonesia, India, Algeria, Kuwait, Saudi Arabia, Russia, Ukraine, Argentina, Chile, and Venezuela. (USTR, 2019)

As a result, seeking action in the U.S. or member countries of the EU is typically deemed preferable, if such jurisdiction is available for the cause of action at hand.

## Conclusion and Recommendations

As Figure 2 depicts, the majority of civil cases settle outside of court. These dismissals, settlements between parties either before or mid-rail, offer an additional benefit – they reduce the burden on the victim organization to reveal sensitive information in discovery.

If information security professionals take anything from this, it should be that they *must spend time with their legal colleagues when establishing and evaluating a data protection program*. Your organization likely has trade secrets worth protecting, and the advice of legal professionals will help with the establishment of necessary prerequisites to support legal remediation in the event of IC loss. Think of this as insurance, not to mention a little extra job security.

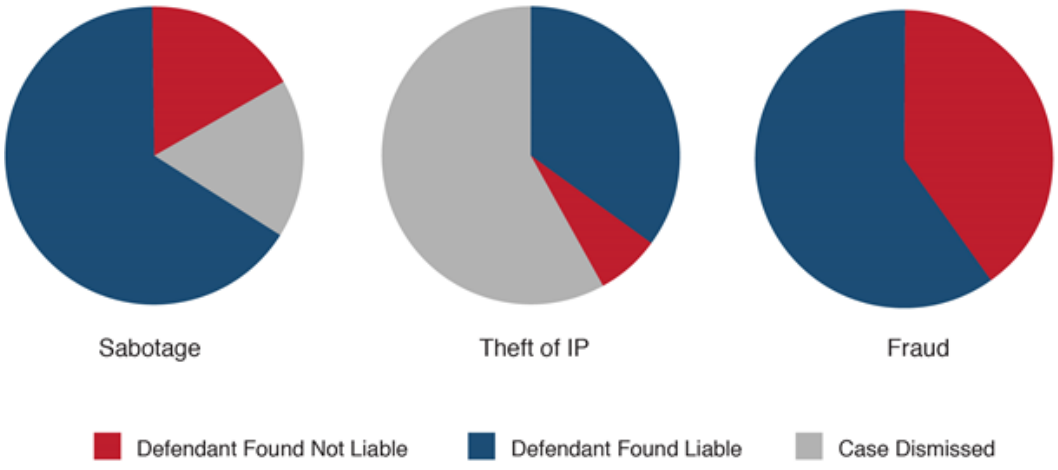
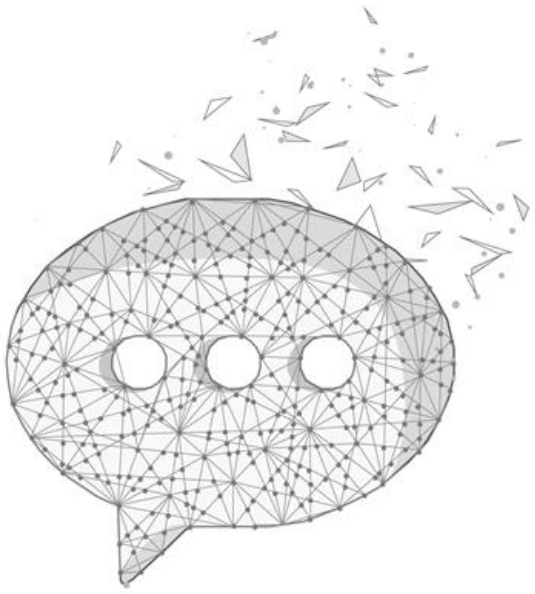



Figure 2. Civil Cases: Dismissal vs. Liability by the Numbers

## Economic and Social Impacts of IC Loss



Given the tight coupling of IC and innovation, when economic and social trends impact IC protection in a specific country, it cannot be assumed that doing business in a market with less intensive IC protections will be the same as doing business elsewhere. Organizations must conduct specific risk assessments for the markets that they operate in and must tailor security controls accordingly. In terms of the negative impacts to individual companies, it's important to keep in mind that there are two significant differences between the damages that a company experiences from the loss of regulated privacy data such as PII, PHI and PCI, as opposed to the loss of IC.

First, the costs of IC loss are more difficult to quantify than the loss of privacy data. In contrast, the loss of PHI, PCI and PII can lead to significant (and tangible) privacy, brand and economic damage, as the impactful breaches of Equifax, Target, Anthem and Home Depot have illustrated (Casey, 2012). These breaches typically result in significant fines, customer loss, reduced corporate credit ratings, C-level firings, and, in the worst cases, significant brand and reputational damage.

Innovation Capital carries a promise of revenue generation, and that value is both contextual and continually changing over time. The theft of IC can impact a company's competitiveness, future revenues, or even long-term viability. This means that even though IC theft has fewer upfront costs, the loss may impact revenue for months or years in the future. It could prevent a company from being first to market, degrade revenue, or result in the loss of an entire line of business or market segment for future operations. Even if calculating the value of IC loss is difficult, it still should be done.

If we take the example of "time to market," being the first to market can dictate market winners and offer significant competitive advantages. The theft of IC or buying stolen IC can seem lucrative and greatly accelerate a company's time to market in addition to the benefits of not having to expend the resources to innovate. As a result, a victim company can lose its early mover advantage if a competitor learns of a

new product launch schedule or pricing figures and can subsequently enter the market first or undercut pricing. The company AMSC had a similar experience as described earlier in this document in the **wind turbine case study**. In this case, AMSC was the victim of IC theft after their largest customer, the Chinese company Sinovel, purchased stolen AMSC IC, used the IC in their products and promptly ended its payments to AMSC. This brazen move resulted in AMSC losing 84 percent of its market cap (equating to about $1 billion) and over half of its global workforce as a result (U.S. Department of Justice, 2018).

The assets most at risk for IC loss are corporate trade secrets not yet in the public domain, business models, process innovations, or pricing and supply chain data. As a real-world example, in 2013 a group of people identified by security firm FireEye as “FIN4” hacked into corporate networks to steal strategic information that could be used to guide financial investments through illicitly obtained insider information (Bennett, 2015). Sometimes this trade secret component of IC is any data that cyber thieves can monetize quickly, but in other cases they can be hard to monetize yet offer a major advantage. For example, an efficient, high-yield biologics manufacturing trade secret may help a competitor, but a cyber thief may not be able to quickly monetize it.

Second, unlike loss of PHI, PII and PCI, each of which carry mandatory reporting requirements, IC theft is virtually invisible. The victimhood of individual organizations goes unnoticed by outside organizations until years after the impact is felt, and then only if it becomes public (usually through law enforcement action), precisely because there is no law, regulation or standard requiring, or providing safe harbor for, organizations to report IC loss. It is understandable that a company’s view of a breach of its defense of IC might focus on proximate interests: customer notification, credit monitoring, legal judgments, regulatory and reputational penalties. There are accepted thumbnail metrics for cyber incident costs like public relations, attorney fees and improvements in cyber defense. However, as we’ve seen, the costs of IC theft are normally indirect or hidden, making them difficult to quantify, such as devaluing of trade name, revoked contracts and lost business opportunities — all of which typically happen over a much longer timeframe as competitive advantages are eroded. This makes them more difficult to quantify than a PHI, PII, PCI breach, although no less important to address.

Given the importance, invisibility and difficulty of quantifying IC loss both to U.S. society and individual corporate entities, organizations should better understand the threats and possible solutions. As with the loss of any sensitive corporate data, the loss of IC can lead to significant economic damage both to the companies whose data is affected as well as the U.S. innovation economy. It is for these reasons that we emphasize the necessary and valuable role Information Sharing and Analysis

Organizations (ISAOs) such as the Health Information Sharing and Analysis Center (H-ISAC) must play. These forums offer members access to a wealth of knowledge and tools that can help prevent an IC breach if properly addressed. Disclosing breaches has moved from a reputational taboo and embarrassment to reinforcing the spirit of sector-wide improvement. Organizations should engage in information sharing practices and cooperative incident response. The level of enthusiasm for this strategy must come from the top down (e.g., a CEO should not restrict a CISO from information sharing during a breach).

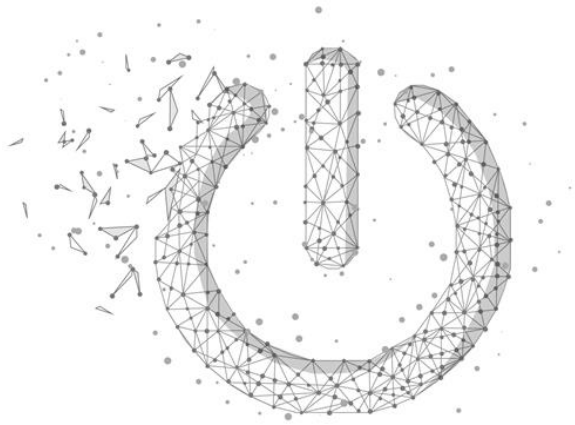
In terms of U.S. society, the most obvious negative impact is that because sensitive data loss weakens corporate entities, the overall economy weakens, leading to lower investment returns, job loss, reduced overall GDP, and lowered overall competitiveness for the nation. As corporate entities make less revenue, they will have less capital to invest in the next generation of workers and solutions that often deliver innovations to market. Thomas J. Donohue, president and CEO of the U.S. Chamber of Commerce, stated that "America's IP is worth $5 trillion. IP-intensive industries account for 38 percent of total U.S. GDP, support 40 million American jobs and drive 60 percent of U.S. exports" (Donohue, 2014). When considering the enormous effect that IC has on the U.S. economy and significant ramifications of IC theft in the U.S., any incident will present unique public policy challenges.

In addition, when the theft of sensitive data provides revenue or market share to corporate or government entities from other countries (e.g., China, Russia), their gains weaken the position of the U.S. both economically and politically in the world. In 2015 the Office of the Director of National Intelligence estimated that economic espionage through hacking costs the U.S. about $400 billion annually. **Case study 4** describes one of the largest state-sponsored hacking campaigns that was ever prosecuted by the Department of Justice. In this instance, nine members of Iran's Mabna Institute, a quasi-government technology company, were charged with conducting a massive campaign to steal IC totaling more than $3 billion from hundreds of American and foreign universities and private sector companies (U.S. Department of Justice, 2018). This case exemplifies the differences in cultural viewpoints of IC theft. Some countries and individuals may view IC theft as patriotic and in some cases these thefts are even state sponsored. As a result, special guidance is recommended for operations in **USTR301** Watchlist Countries (Office of the United States Trade Representative, 2018). An example of this may be enhanced mobile/laptop protections when employees are traveling in these countries where there are operations.

As a critical infrastructure designated industry, the healthcare community must maintain a high quality of compliance and service delivery throughout its value chain. To healthcare providers, pharmaceutical and medical device manufacturers and

insurance providers, IC is a crucial component to public safety and consumer confidence. Strong IC protections and enforcement are important to preventing potentially harmful products, such as counterfeit pharmaceuticals, from reaching consumers' hands. In a 2017 update to the IP Commission Report, it is stated that the estimated cost to the U.S. economy "continues to exceed $225 billion in counterfeit goods, pirated software, and theft of trade secrets and could be as high as $600 billion" (The National Bureau of Asian Research, 2017). However, these figures do not account for the full cost of patent infringement.

# Information Protection Control Recommendations



While healthcare organizations can generally demonstrate diligence by implementing foundational cybersecurity controls[3], as the case studies we've outlined show, foundational controls alone are insufficient to adequately protect an organization's IC. To the extent this is true, the recommendations below assume foundational controls such as a risk management program, malicious code protection, intrusion detection systems, security incident and event monitoring systems, a secure development lifecycle and firewalls, and other controls are already in place.

We do not attempt to repeat cybersecurity control guidance provided elsewhere around these control types. Rather, the focus here is on those additional, contextually relevant controls that maximize organizational protection against loss, exposure and adversarial action to IC-related objectives.

Below, we outline the additional controls relevant to the themes discovered in previously outlined case studies and the extended detective, protective and administrative controls necessary to secure IC in multiple contexts (physical, technical, administrative, and legal). We have included control introductions, control recommendations and implementation guidance with major control areas to assist the reader with understanding some of the affirming elements and challenging aspects of a particular type of control implementation. Where warranted, implementation guidance is provided in certain subsections.

## Controls Overview

At the highest level, an effective cybersecurity program must be comprised of two elements: an inventory of assets classified according to value and a catalog of implemented controls and capabilities that are managed and tracked for maturity and mitigation effectiveness.

When a cybersecurity program is fitted to address IC risks, these elements retain their importance, but must be carefully extended

[3] e.g., Risk management, malicious code protection, vulnerability management, perimeter access control, SSDLC, phishing protections, etc.

to cover the distinctive challenges posed by IC protection in the physical, logical and administrative contexts. As outlined in the introduction, the example base structure below summarizes the main areas of focus for an IC protection program, each of which are described more extensively in the subsections that follow. To illustrate, simplify and underscore the necessity for comprehensive and aggressive approaches and a national posture toward the protection of individual and national interests in the protection of IC, we have characterized the control recommendations available to healthcare organizations for application in their environment into two main categories:

1. **Passive Measures.** These include elements such as governance and oversight, policies and procedures, awareness and training, communication, audit, artifacts of employment acknowledging the importance of protecting IC, rightful ownership of work product, etc. These are artifacts necessary to make cases, but do not directly prevent or preclude loss, exposure or theft.

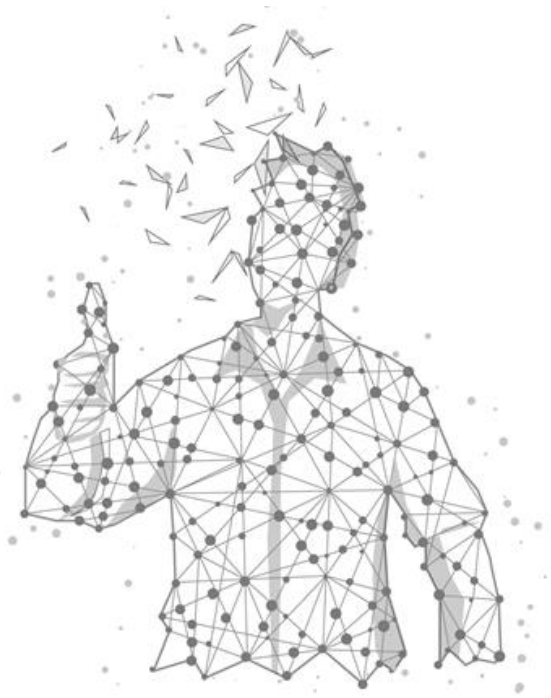
2. **Active Measures.** These address the problem of detection and prevention of loss, exposure and theft. The active measures discussed below largely refer to and involve the use of technologies, preventative and detective controls, applications, and practices for information asset identification, disposition for protection, lifecycle management, threat intelligence practices[4], and data control. Asset examples are provided for the sake of clarity, including but not limited to IC protective controls that in some cases may exist as a subset of recommendations in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF): e.g., data loss prevention in motion and at rest [5], identity and access management controls, centralized control (or elimination) of removable media, encryption of removable media, digital rights management, and other approaches.

Across both control types, it is important for organizations to keep current with technical and non-technical trends as part of your periodic review and sustainment efforts. There are numerous ways for organizations to accomplish this, and it starts with making the time investment to engage and collaborate externally. Be it through your partners, peer forums or public-private partnerships, the sharing of lessons learned is integral to maintaining a current state of readiness across your organization's control measures.

[4] For additional information, see the Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO) produced by the HSCC CWG at https://healthsectorcouncil.org/hic-miso-pdf/

[5] This is also described on page 47-50, Tech Volume 2, of the Health Industry Cybersecurity Practices recommendations found here: https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf

## The Human Factor and Control Implementation



When implementing defensive control options, it becomes important to simultaneously consider how the various actors (persons, organizations, nations) might act on IC objectives, and also to carefully consider how exacerbating requirements (such as privacy considerations) might affect control implementations.

**IC threat actors can generally be placed into one of four categories:**

1. **Insiders, through inadvertent disclosure or casual action**[6] People handling data, directly or through system management, may accidentally disclose that information. Common examples include IC in an email sent to the wrong person and unsecured IC in databases that are exposed to the internet without access control. Workers may casually appropriate information they deem useful to them in their next role as they prepare to leave a company. This type of actor likely will not regard their actions as theft, mixing company protected IC with personal data. Such employees are generally interested in reference material to showcase their prior works, or to avoid repeat work in the future, inconsiderate to the business value of the IC or the potential ramifications of their actions. And to the extent that they work in a country, state or region with stringent privacy laws applicable to employees working on company premises, company equipment and company time, such companies may yet find themselves with significant headwinds toward implementing the full suite of IC safeguards.

2. **Insiders, through theft**[7] Workers may see financial or professional value in the information accessible to them and intentionally seek out, collect and retain IC for their own use. These insiders are far more likely to circumvent technical controls and to collect information beyond the scope of their job

[6] **https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf**, p 22

[7] **Ibid**, p. 20

responsibilities. Typically seen with exiting workers, examples could include a scientist who wants to bring a record of compounds and test results to their next employer, saving research effort, or the corporate strategist who keeps company long range plans when changing jobs to direct the strategy of their next employer. Though less common, this also includes insiders who stay employed at one company but provide IC to third parties for their benefit. One notable IC theft case study is an example of that ongoing theft scenario. As these insiders are deliberately stealing IC, compared to casual theft, there is an increased likelihood that the theft will result in business impact.

3. **Outsiders, through malicious action.** Various external actors, ranging from hacktivists to national intelligence agencies, are incented to gain illicit access to corporate IC and have specific adversarial objectives at the outset. These threat actors will, by definition, need to bypass one or more technical controls to accomplish their objectives without any authorized access to company IC. These attacks often involve the use of phishing, stolen/hijacked credentials, or necessitate the recruitment or placement of insiders.

   Defensive controls may need to be tailored to each category to be effective. For example, a real-time warning pop-up may stop accidental disclosure by an employee; however, it likely will not deter a motivated adversary.

4. **Third Parties and Business Partners Through Inadvertent Exposure, Casual Action, or Lack of Control Parity.** Professional services firms, contract workers and managed service providers are often provided direct or indirect access to company IC sources, but may not be trained in the same way, handle it in the same way, or have the same sort of control structures in place to support the protection of data. This places a heavy burden on hiring organizations. Each type of system and data access, method of data transfer and handling method associated with the work of such third parties must be carefully vetted to ensure an appropriately risk-tolerant control structure.

## IC Protection – Passive Measures

Organizations of all sizes working with IC, producing IC, or providing services to IC generating healthcare companies, should implement a multi-pronged Govern, Train, Attest and Control (GTAC) approach to protect themselves and their foreign and domestic business partners from IC theft, loss and exposure.

**Caveats**

It should be noted that where policy recommendations are listed below, we are not taking a specific position on the number or grouping of policies within an organization. We are only recommending these be documented as *statements of intent* within one or more policies within an organization.

The following passive controls are recommended to improve IC protection at healthcare organizations in-scope for this document.

### Information Asset Governance

1. **Information Asset Management Program Governance**

   A strong information asset management program begins with policy pronouncements that require a continuously updated and detailed list of all key information assets and the systems within which they are created, managed, stored or transmitted.

   Further, it should articulate some level of understanding for the qualitative, if not the quantitative, value those data represent. The heart of this governance is an artifact referred to herein as a data map that articulates sources, destinations and methods of transfer for the subject data. Clearly, if an organization doesn't define what it possesses, where that is, who owns it, or the methods by which that data is properly moved, copied or altered, it will find the effective management of that data difficult, and protection against IC loss more so. Developing such a data map can be done through manual or automated means but is typically achieved through a blend of both.

   Recommended governance components in this area include:

1. Information Management Policy Statements, including:

1.1.1. The definition of information assets.

1.1.2. Requirements for development and continuous maintenance of an information asset inventory and data map with the following attributes:

1.1.2.1. Systems and repositories which contain IC

1.1.2.2. Data/Information sources and destinations

1.1.2.3. System owners

1.1.2.4. Data owners

1.1.2.5. IC sensitivities

1.1.2.6. Laws, regulations, standard references

1.1.3. Requirements for periodic valuation of inventoried IC.

1.1.4. Assignment of accountabilities for maintenance and periodic valuation of inventoried IC.

1.1.5. A defined information asset lifecycle.

1.1.6. Handling requirements for defined sensitivity levels.

1.1.7. Requirements for procedures for the destruction of data.

1.1.8. Requirements for clearing remnant data.

1.1.9. Rules regarding disposition of orphaned data/systems which take sensitivity levels into account (e.g., Policy restrictions or pronouncements on use of applications and modalities which place sensitive information in unmanaged states).

1.1.10. References to standard procedures for collection and preservation of information upon termination.

***Something to think about…***

**The indictments in Case Studies 1 through 3 highlight the important of DLP, but it is worth noting that *effective* use of DLP is predicated on existence of policy requirements for (and the instantiation of) a comprehensive information asset inventory and wide-spread labeling of sensitive data.**

1.1.11. Staff in highly privileged roles will have enhanced monitoring emplaced on their credentials and work activities.

1.2. Information Classification Policy Statement, including:

1.2.1. Classification of IC (by type and by sensitivity).

1.2.2. Ownership of IC.

1.2.3. Rules for handling IC in all forms.

1.2.4. Requirements for labeling of IC.

1.2.5. Limitations on access.

1.2.6. Limitations on transmission and storage.

1.2.7. Assignment of accountability for classification changes.

1.2.8. Examples of IC.

1.2.9. Requirements for periodic training for sensitive data handlers.

1.3. Periodic audits of IC protection protocol adherence

1.4. Sanctions for violations of program governance

**Implementation Guidance**

Once the data map is completed, an organization should undertake a specifically cyber security classification of those same assets (data and systems) for the purposes of targeted protection, handling, and monitoring mechanisms. Although there is no off the shelf classification method that delivers absolute protection to address all present challenges[8], a thoughtful approach, properly implemented and accompanied by supporting active protection measures, achieves significant protection for data (at rest and in motion) not otherwise possible.

[8] Challenges likely to be encountered include, but are not limited to, over-classification, classification clustering, and under-classification.

Secondly, while classification types may vary from organization to organization, in general, all organizations should begin by classifying both structured and unstructured data under at least three levels: confidential, internal use only, and public. Beyond this, and to fit certain industry and organizational requirements, a fourth level (restricted, or similar) is sometimes added to identify highly sensitive information meant to address the most important corporate data. When this fourth level is then linked to role-based access and compartmentalized, the best outcomes may be achieved. Although examples of this type of compartmentalization might also include material non-public information such as mergers and acquisitions, plans for reductions in workforce, or predictive models for informing corporate strategy, only the last of these would be considered IC.

***Something to think about…***

Case Study 1 demonstrates the importance of program governance, signed artifacts, periodic training and reminders on the proper handling of proprietary information. Without these things, employees and contractors acting in good faith may be left unaware of the risks. Further, making a case against rogue employees or contractors would be deeply complicated at best. An annual process is an effective way of ensuring that people are aware of expectations and that the corporation can demonstrate the awareness.

As noted in case study 1, visual classification labels are an excellent component of data security as they can guide correct behavior by ensuring (1) that sensitive documents are recognized as sensitive by authorized users (2) that any misappropriated documents are recognizable as sensitive company information by any third party that encounters them and (3) that active controls, such as DLP, are able to key off these classification labels, thus amplifying the effectiveness of both.

Finally, the policy statements outlined above can be documented in one document or multiple as appropriate for the organization. These policy statements, as published, should be accompanied by the necessary communications and awareness to ensure compliance across any functions that create, update or handle IC.

## Workforce Agreements

### 2. Terms of Employment

Although it is broadly and generally accepted that adherence to company policy is a condition of employment, it is not universally the case that healthcare companies issue specific and standalone artifacts to employees to separately highlight the importance of protecting IC or articulate the sanctions arising from a failure to do so. Moreover, it is often the case that third party workers such as contractors, consultants and managed service providers are expected to be covered by non-disclosure agreements that may not specifically require the return of any

original works developed in service of the company that hired them (such as a failure to include a proprietary innovations and information agreement).

2.1. Proprietary Innovations and Information Agreement(s).

2.1.1. Applicable to both company employees and contingent workers.

2.1.2. Individually signed upon hire or contract execution.

2.1.3. Periodic Reminders to employees and contingent workers of their obligations to turn over any innovations to the company that are produced on company time, or using company assets during the period of their employment or contract.

2.2. Confidentiality and Non-Disclosure Agreements (CDA/NDA) Advisable Components.

2.2.1. Individually instantiated CDA/NDAs with all third-party staff and subcontractors developing, storing, or handling innovation capital.

2.2.2. Signed upon engagement or hire, and clearly indicating that no company secrets or IC will be revealed to any other individual party not specifically identified to receive it by the company.

Other advisable components of a program with non-disclosure components include:

2.2.2.1. A repository for storing electronic records of such agreements and their participants.

2.2.2.2. Periodic reminders or training outlining CDA/NDA requirements.

2.2.2.3. Limitations on badge use (e.g., prohibiting another to use one's badge to enter an area otherwise restricted under non-disclosure or confidentiality agreement).

2.2.2.4. Limitations on Photography, Audio, or Video recording or devices which have these features.

2.2.2.5. Prohibitions on reversing software or hardware components.

2.2.2.6. Limitations on sampling protected IC.

2.2.2.7. Limitations on copying source code or samples of source code.

2.2.2.8. A method for reporting violations.

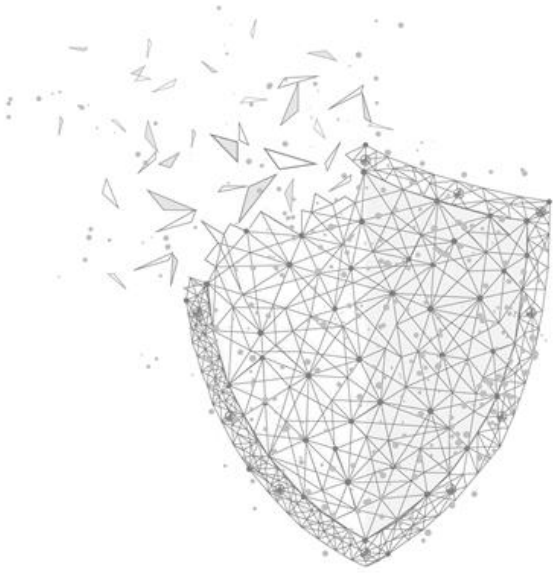
2.2.3. Conditions for third party/contingent workforce employment.

2.3. Sanctions for violations of contract or employment terms.

**Implementation Guidance**

Given that the agreements outlined above tend to be signed at employment or contract execution, some organizations may choose not to effect a secondary document such as a 'proprietary innovations and information agreement' but rather, to include the terms and conditions associated with such an agreement inside the employment contract or statement of work. This is perfectly acceptable; however many organizations separate them for the purpose of underscoring the importance of each separately and consistently. Also, given that these documents are signed at the point of employment, it is beneficial to consider regular reminders to help with adherence and enforcement.

## Physical Security Policies



### 3. Physical Security Policy Statements

Physical security provides a necessary foundation upon which to build and maintain other types of access controls. Physical security exists beyond the gates, bollards and contract security guard workforce; it exists at manufacturing plants into which staff and contractors carry smartphones with high resolution cameras, advanced audio recording capability, video and an independent exfiltration mechanism (i.e., a 5G data network). For sensitive information processing and trade secret protection, advisable physical security policy components include:

3.1. Restrictions on access to areas where IC is developed, maintained or stored.

3.2. Procedures for the periodic review of access lists to such areas.

3.3. Use of inventoried and controlled identifying tokens or badges at key control points.

3.4. Limitations on use of personal smartphones, cameras, audio or video recordings in IC processing facilities.

3.5. Limitations on storing hard copy IC, printing, filing and clean desk requirements.

3.6. Specialized procedures and guidance for employees and company sponsored contractors traveling to high risk markets such as might be identified in USTR301 Priority Watch Lists[9], or elsewhere.

3.7. Sanctions for violations of Physical Security Policies and Procedures.

### Implementation Guidance

Physical and digital signage in high traffic areas (e.g., conference centers, cafeterias, entrance lobbies) are great mechanisms to remind the workforce and reinforce the controls outlined in the policy statements. Additionally, staff should be strongly encouraged to report known or suspected violations to security staff for follow-up.

[9] See **https://ustr.gov/sites/default/files/2019_Special_301_Report.pdf**

## Restrictions on Systems and Information Use

### 4. Acceptable Use Policy (AUP) Statements

Although the policies may be named something different at each company, acceptable use policies typically define the appropriate and inappropriate uses of company networks and systems. Advisable policy requirements for the protection of IC include:

4.1. Restrictions on the movement of company or partner IC to unauthorized external locations or personal devices.

4.2. Restrictions on opening company IC into non-company managed[10] applications.

4.3. Policy restrictions on use of unauthorized backup services[11] for mobile devices, desktop systems or server infrastructures.

4.4. Policy restrictions on inappropriate or untimely deletion, or activities which might complicate discovery, collection or archival.

4.5. Restrictions on installation or use of software or SaaS applications not specifically designated required for business purposes.

4.6. Clarifications on corporate monitoring and Active Controls (e.g., Data Loss Prevention) to ensure workers are transparently advised on monitoring of the access, modification and transmission of IC.

4.7. Limiting photos of internal company processes, systems, information, and process development operations.

4.8. Obligations to protect information upon voluntary and involuntary termination.

4.9. Restrictions on access to company networks, systems and information to company managed devices.

4.10. Associated Device Agreements to address restrictions & collection of corporate mobile and desktop computer devices upon termination of employment.

[10] Managed refers to approved applications under the control of a company mobile device management (MDM) solution.

4.11. Review and acknowledgement by all employees, contingent workers and third-party service providers with direct access to corporate systems or hardware.

4.12. Sanctions for violations of AUP terms.

**Implementation Guidance**

Within any acceptable use policy, it is important to clearly articulate that all monitoring, collection, incident response and investigations will be conducted in accordance with local law. It is also important to directly reference the company's code of conduct (or equivalent) as an important governance mechanism.

## Workforce Engagement and Training

5. Awareness and Training for employees, contingent workers and relevant third-party service providers regarding common IC protection methods:

5.1. Tips and tactics to defend against social engineering.

5.2. Tips and tactics to recognize and defend against phishing/spear-phishing.

5.3. Restrictions on copying, or transferring original data, source code, files, or devices in whole or part.

5.4. Rules regarding printing and destruction of sensitive content.

5.5. Restrictions on photos, audio, and video recordings.

5.6. How to spot and report IC theft or indications of theft.

5.7. Consequences of IC Theft.

5.8. Sanctions for failing to complete awareness or code of conduct training.

**Implementation Guidance**

For international organizations, it is important to verify which language translations are required for awareness and training content. Enforceability is very dependent on the assurance that awareness, training and associated communications were made available in local languages, where reasonable. Consult with legal to confirm which languages are required.

Individuals learn in different ways, so it's highly recommended to offer multiple methods of awareness and training; this could include web sites, videos, push alerts, e-mail reminders, games and posters.

## Third Party Risk

### 6. Supply Chain and Third Party Overnight

Third party processing of IC presents one of the most significant and challenging risks to any organization. Healthcare organizations typically rely on third parties such as contract manufacturing organizations (CMO), contract research organizations (CRO), inter-company partnerships, staff augmentation, consulting organizations and process development contractors to assist with development, handling, storage or modification of IC. Organizations must therefore have a plan for onboarding, assessing, contracting, active monitoring and offboarding third party partners. Such third parties should be continuously evaluated to ensure controls sufficiently protect IC at a level commensurate with the hiring organization's control investments. Third party oversight programs for IC generating organizations should consider the following components:

6.1. Policy statements mandating third-party qualification and prerequisite security assessment for partners which either access, host or exchange IC.

6.2. Consistent and centralized due diligence processes (where feasible) to assess and determine appropriateness of controls, commensurate with the data in scope of the engagement.

6.3. Contract terms should have an information security schedule attached which address general cybersecurity safeguards, but also specifically identifies active and passive controls that protect IC.

6.3.1. Contract provisions for periodic security assessment.

6.3.2. Requirements for control parity[12] (maintenance of control parity assured through periodic reassessment).

6.4. Governance and active monitoring.

[12] Control parity refers to relative protection level of third-party controls to their reference control in the contracting party's control structure

6.5. Standards for access, connectivity and collaboration, as well as off-boarding.

6.6. Provisions and controls for third-party contingent labor (MSPs, BPOs, etc.).

6.7. A protected sourcing/contracting data store which identifies third parties which produce, store or access critical IC.

**Implementation Guidance**

Supply chain and third-party risks extend far beyond just IC protection. It is important to partner with other relevant stakeholders to ensure supply chain and third-party risk triage, assessments and other related processes are aligned across key functional areas such as procurement, legal, ethics and compliance and quality.

Governance for third party monitoring must be a cross-functional effort, which includes law, sourcing/procurement, audit, information security and business functional representation. Recognizing that innovation capital protection is but one dimension of concern that might arise with a third party, it is important that communities of interest within one's organization are committed to applying sanctions against contracts that fail to address those concerns, up to and including termination of a contract relationship. It is also important that this community of interest have a regular forum within which to express and report out on metrics and concerns related to those third parties.

## Incident Management

### 7. Security Incident Response

Although many of the controls outlined in this paper help mitigate the risks of IC loss, exposure or theft, incidents will happen. While administrative, detective and preventative methods are indeed vital, it is equally important to ensure the necessary response and recovery procedures are in place, and that they specifically consider IC protection scenarios.

Incident response policy components for IC loss or theft should include:

7.1. Requirements for integrated incident process testing with a focus on loss, exposure and theft related incident types.

7.2. Mandates for corrective action reports or observations, with follow through and cross functional sponsorship.

7.3. Periodic joint review of the IR policy and processes for efficacy in the resolution of IC related incidents.

7.4. Requirements for functional membership in the incident response team (particularly in response to known or suspected IC theft) by representatives from Information Security, Human Resources, Privacy, Employment Law, and IP Law at a minimum.

**Implementation Guidance**

Each organization should document the major types of incidents and the corresponding response procedures. Three common types of incidents that warrant separate procedural coverage and steps include:

**Operational Impact.** Incidents that slow down or stop IT networks or systems, directly impacting the accessibility and availability of applications and data. These are triggered through vectors such as malware, ransomware and denial of service attacks, etc. and rarely target IC directly.

**IC loss, Exposure or Theft.** Often triggered by Data Protection controls as outlined in the Active Measures section, these incidents could directly relate to IC protection. Often, data owners must be consulted to gauge business impact. Many of these incidents are based on careless data handling with no malicious intent. However, Legal and HR may be required if an employee or contingent worker is complicit or actively involved in the theft or exfiltration.

**Breach.** In many jurisdictions, a breach is a reserved legal term, and is normally limited to incidents where the data is in scope of regulatory mandates (e.g., PII, PHI). Given that breaches often require disclosure, Public Relations, Corporate Communications and other enterprise stakeholders must be engaged during response and recovery.

Incident response tabletop exercises should also challenge organizations to respond to IC theft scenarios with employee privacy, insider and nation state dimensions to them. During the response and investigative activities for any of the incident types described above, if an individual is targeted for forensics — whether it's their email activity, internet usage or application access, security teams must ensure a process is defined in advance and takes HR and legal advice into account. Data privacy officers may also require consultation in the EU and other jurisdictions with stricter personal privacy regulations.

# IC Protection – Active Measures

The ability of each organization to implement active protection measures within their environment will vary based on capacity for investment and organizational maturity. However, all organizations should consider implementing each item outlined in this section. Foundational to the effective implementation of these controls is the establishment of the complementary passive measures described in the previous section.

## Information Asset Management and Risk Classification

### 1. Asset Discovery and Information Classification Tools

Tools for periodic asset discovery, as well as ongoing risk assessment are cornerstones to mitigating risk of loss, exposure, and theft. Once these have been established, classification should then be attached to the information via metadata attributes, visual labels or other indelible marking. Such markings can be used to assist users in managing the information properly, as well as enabling protective technology (i.e., DLP) to efficiently identify such content, and apply the appropriate control structures. At a minimum, large and medium sized organizations should actively consider deployment of tools that perform:

1.1. Periodic information asset discovery/inventory of systems and data.

1.2. Classification (both manual and automated).

1.3. Continuous (automated or scripted) disposition.

1.4. An Information Management and Classification Training Program(s).

**Implementation Guidance**

Organizations should strongly consider implementing a capability that allows for classification upon creation and automated information tagging/classification to ensure proper identification and protection of IC in motion, and at rest, proactively and retrospectively. As classification on creation (in particular) represents an extra step in day-to-day ways of working, organizational change management must also be adequately planned for and established. To be sustainable and effective in the long term, a data classification program must have clear expectations negotiated and agreed upon between those who protect the data and those who lead data creation, with a shared sense of purpose at the outset. It also requires significant and consistent executive sponsorship. Without the highest levels of executive leadership in full support, such a program is likely to find itself in retrograde before it has achieved its promise.

### Caveats

No small part of data classification program efficacy is directly tied to the relative level of awareness, understanding and practice of content/data creators. They must choose the appropriate risk category for the documents/content, and assist in its continuous and proper disposition. For this reason, both over classification and under classification are common. This underscores the necessity for ongoing education and awareness campaigns. Moreover, classification on creation does not address remediation of assets that have already been created without a classification tag, and therefore retrospective classification (using machine learning, templates and keywords) must be addressed separately.

## Identity Controls

### 2. Identity and Access Management (IAM) Controls

Robust access controls are fundamental to IC protection. In scenarios of loss, exposure or theft, data at risk will first likely be actively limited by access control. In principle, such access should be limited to "need-to-know," and based on the individual's role within the organization. It should also be possible to re-trace a particular entity's action through a system and potentially integrate it with risk-based administrative decision trees. Therefore, key elements of a robust IAM program include identity stores, authentication mechanisms, authorization management, and auditing controls. This overall integrated system of controls ensures a given user must validate their identity (usually with secrets known only to them and/or other pre-configured credentials, limits their permissions based on role, discretionary accesses or both, logs such access to various resources, accounts for the same as necessary, and provides a trusted verifiable (auditable) trail of action. IC is virtually always protected by some combination of IAM systems, and sometimes multiple. Technologies such as Microsoft's Active Directory, the open source Samba project, Lotus Notes or even simpler local-system user management technologies are all used in this capacity. The maturity, integration, robustness and granularity of the system can vary widely. IAM is based on four main components:

***Something to think about…***

Case Study 1 demonstrates how, as part of an IAM program, limiting access to information pertaining to company products (and products under development) to which employees are not assigned, is fundamentally necessary to protect IC. Limiting sensitive information access to only those roles cleared to work on specific classification levels and products is referred to as 'role based' security'.

For example, a Protein Researcher might justifiably be granted access to all protein research and related manufacturing processes vs. just those for a specific product he or she is working on (since all of that information might be job relevant) RBAC limits access to such information by all *other* employees based on their limited or nonexistent need to know it.

**Identity:** who an individual is, and their attributes (e.g., job title, department).

**Access:** the ability to access an application, system or other resource (e.g., file share repository).

**Authorization:** processes and/or decision checkpoints to allow or disallow a particular depth of access, usually based on user attributes, groups, roles, etc.

**Auditing:** verifiable processes which track, document, and measure usage, and activity for a given user or process which has been authenticated and/or authorized.

Key IAM elements most directly relevant to IC protection include:

2.1. **Entitlements.** An appropriate set of baselines[13], and extended access privileges based on identity attributes and/or roles.

2.2. **User Authentication.** The strength of the authentication, including the type of credentials required, should not only be based on a confirmation of the proper credentials of the individual, system, or process, but also the observed risk level[14] posed by the authenticating identity.

2.3. **Device Authentication.** Allowing only company managed devices to attach to the company network or application.

2.4. Monitoring of successful and failed authentication of devices and users.

2.5. **Federation.** Trusting a separate, authorized source to confirm the identities and authenticate accounts, before allowing access.

2.6. Robust role and discretionary based access management/authorization for IC. Access authorizations should be:

2.6.1. Classification based.

2.6.2. Product based.

[13] Baseline entitlements, sometimes referred to as 'birthright entitlements', refer to the minimum privileges required to effect productive access.
[14] Solutions extant for risk-based authentication are increasingly common, and take into account previously observed and unobserved behavioral (time, geography, concurrent logins etc.) indicators for individual identities.

2.6.3. Role based.

2.6.4. Periodically reviewed, with higher frequency reviews for administratively privileged and IC authorized roles.

**Implementation Guidance**

We strongly recommend that IAM services, including the provisioning and deprovisioning of access, be performed within the security function, separate from shared IT services such as the help desk or infrastructure operations. This ensures that access and authorization maintain a healthy tension with availability, and that one of the integral elements of active IC protection is not unwittingly sacrificed for temporary and potentially less valuable interests.

Because HR owns the human capital processes for the organization, which forms the basis of identity inventories, the team responsible for IAM must also be very tightly partnered with that function. HR also must trigger employee identity lifecycle changes to the IAM team, as employees change jobs or are terminated. Accountabilities should be confirmed in this area, especially when considering contingent workers and outsourced partners.

For contingent workers and third-party service providers, it's imperative that notifications of job changes and/or terminations are made in a timely manner so access controls can be adjusted or deactivated accordingly. This should be enforced via contracts, strong oversight and aggressive monitoring of such programs with third parties, as outlined in the supply chain and third-party oversight section in Passive Measures.

Federate, wherever possible, to trusted sources for authentication. Companies should not duplicate the identity creation for external partners or third parties, as they will not have direct visibility to their status or position. These external federation standards should be based on trust levels, which in turn are based on variables such as device, user authentication credentials and data classification.

Actively segregating systems processes and identities that handle IC and enforcing security boundaries/access control between them using established security models such as Bell-LaPadula are the aspiration of every IAM program. Whether in the logical or physical security realm, IAM programs should take care to balance this north star design principle with user experience to ensure sustainability.

## Data Controls

### 3. Data Protection

There are numerous technology and process controls that should be employed to protect IC. These tools require active governance and management to achieve risk mitigation. With finite resources, organizations will need to prioritize which controls will provide the most value, given the business model(s) specific to the company. Additionally, there are some governance elements, processes and data handling principles that should be actively enforced. These include:

- A well-resourced monitoring program, which can trigger incident and response activities, as necessary.
- Documented file storage and data transfer standards (e.g., cloud file storage partners), and monitor for unapproved methods.
- Active tuning and automation for discovery, identification and classification rules.
- Continuous review of IT assets to ensure 100% coverage.

***Something to think about…***
Case Studies 1 through 3 demonstrated the necessity and value of DLP technology which, when combined with Classification labeling/metadata, form matching, exact data match (EDM), heuristic keyword matching, network movement and multiple other techniques can stop unauthorized transmission of intellectual property data to external email systems. While DLP alone does not provide complete protection against theft, it is a crucial layer, and is noted as a critical point of failure in the Case Study 1 indictment. In that case, a scientist exfiltrated Trade Secrets by sending them to a personal email account. DLP can silently *stop* such transmissions, warn management, or prompt the user to confirm there is a valid business purpose, curbing theft and increasing awareness.

#### 3.1. Data Loss Prevention (DLP)

DLP, as its name suggests, is a technology control that monitors, detects and if so configured, will block activities that put IC at risk for loss, exposure or theft. It is a powerful method to detect unusual data flows, such as transmission of a Trade Secret to an external email system. Most DLP solutions have an endpoint component, and are pre-configured to recognize high risk data movement patterns, such as writing to removable media, posting to social media, emailing to personal addresses, etc. Some solutions also scan the content to make judgments on the risk level of the data, and trigger controls accordingly. DLP can be configured to simply log risky activity, warn users, or block the activity outright.

The practical realities of multiple business operations contexts, collaboration systems and third-party partners, means that DLP often may be limited in its ability to outright block the

transmission of sensitive data to an unsafe contexts. DLP is also costly and time consuming to implement, and will generate false positives[15]. When properly maintained however, it is one of the more potent controls available for the active protection of IC.

Recommended components include:

3.1.1. DLP monitoring of access to IC.

3.1.2. DLP monitoring of modification to IC.

3.1.3. DLP management of movement of IC via the network, labs, process development, and manufacturing environments.

3.1.4. DLP blocking and/or warnings on movement of IC to removable media, which notify both security and the immediate supervisor of such attempts, whether successful or not.

3.1.5. DLP and Mobile Device Management enforcements to prevent copying company data to personal devices.

3.1.6. DLP Exact Data Match (EDM) for sensitive, and/or structured information types and records.

3.1.7. Technical controls to prevent opening company IC into unmanaged applications or uploading to unsanctioned web apps.

3.1.8. Sufficient staff to monitor access to IC and manage control effectiveness (IC data sources, false positives)

[15] Exact Data Match (EDM) provides an exact reference copy of IC, and goes a very long way towards reducing false positive rates. Organizations should consider this particular implementation type carefully whenever possible.

### 3.2. Digital Rights Management (DRM)

DRM applies access controls, activity visibility and usage restrictions directly within the file itself. The primary benefit is that these controls persist no matter where the file gets transferred, copied or sent. Other controls (e.g., DLP) operate quite well within an enterprise, but control is lost once the file leaves the environment. The two most powerful and widespread applications of DRM technology are Apple's iTunes and Netflix, where the audio/video content retains its access control no matter where the files are downloaded. While technological protection measures have underpinned the licensing of copyrighted works in the digital environment for decades, for enterprise use, DRM is still in relative infancy as it relates to the protection of IC. However, with the commitment and resources to deploy and manage it, DRM is an active protective control structure worthy of strong consideration.

> ***Something to think about…***
>
> DRM can provide more granular control, aside from just protecting against unauthorized users. An authorized document reviewer, for example may be prohibited via the DRM technology, from saving a copy of the document.

### 3.3. Cloud Access Security Broker (CASB)

Many of the impactful security controls upon which companies have depended for visibility, activity monitoring, usage controls and data access or movement have a fundamental flaw; they assume the endpoints, network and systems reside within the enterprise. With the rapid progression and widespread adoption of cloud services, and the growing adoption of bring-your-own devices and a remote, mobile workforce, these controls may become glaringly inadequate. CASB introduces visibility, monitoring and data control for application usage and data access scenarios that occur almost completely on the Internet as a third-party service. For organizations where IC is stored or accessed via these cloud/internet scenarios, CASB can provide impactful risk mitigation. The following CASB control elements are recommended:

3.3.1. Restrictions on data movement and transfers to cloud services based on the account being used (e.g., corporate accounts vs. personal accounts).

3.3.2. Visibility, monitoring and restrictions on usage of non-sanctioned cloud applications or services.

3.3.3. Restrictions on data movement, transfers, downloads and opening of company files based on the status of the device being used (e.g., corporate device vs. personal device).

3.3.4. DLP-type controls for movement, transfer or download based on the risk classification and/or content of the files[16].

### 3.4. Removal Media Control

As described above in the DLP section, copying or transferring IC to removable media is a very common vector for loss, or theft. Given the small form factor, removable media is very easily dropped, falls out of pockets, and can often be accessed from any device. All organizations should give careful consideration to:

3.4.1. Eliminate the use of removable media wherever possible.

3.4.2. Document and track any exceptions to the above.

3.4.3. Inventorying use and placement of such devices should be carefully, but strongly considered.

***Something to think about…***

In Case Studies 1 and 2, a substantial IC trove was copied to portable media devices, and subsequently exfiltrated from those organizations. While eliminating portable media usage represents the strongest security measure for such a risk, a forceful backup control can be found in the form of certificate-based encryption. Certificate-based encryption could ensure that the contents of the media device are both encrypted and can only be viewed on an authorized company asset. This can effectively "lock in" data to the company's ecosystem and limit theft even by company insiders.

3.4.4. Implement make/model restrictions for USB drives to limit unauthorized use.

3.4.5. Implement certificate-based encryption where possible.

3.4.6. Ensure encryption algorithms for USB storage are of strength equal to or greater than AES-256 where exceptions exist.

#### Implementation Guidance

Leading DLP and anti-virus products can implement restrictions on movement of data to removable storage, or block the mounting of these devices entirely. Where exceptions for need exists, encryption can be enforced by and implemented within the operating system, or endpoint protection layer. Exception processes should be clearly established for scenarios where removable media is the only option; these exceptions should only be granted for short periods of time, and all approvals documented as acceptance of the risk. A limited, and inventoried range of secure and encrypted USB drives should be made available for these exception scenarios.

[16] Practitioner beware: Vendors and technologies in this space continue to struggle with scalability of this particular control recommendation. Although it should be leveraged, take care to understand the scalability limits of the vendor in use prior to implementation.

### 3.5. Physical and Logical Enclaving of IC

Highly sensitive IC can be isolated either logically or physically to separate networks, therefore requiring a separate control checkpoint to traverse and access. Often referred to as network enclaves, this is an effective control for protecting this data, but is typically a costly option with considerable complexity.

### 3.6. Encryption

The primary risk that encryption mitigates is unauthorized physical access, either via theft of a mobile device or laptop, or from an administrator within a cloud platform. All laptops and mobile devices should be encrypted as a default, fundamental control. The best combination of protection and minimal performance impact is usually achieved when encryption is enabled at the hardware or OS layer.

Sensitive IC stored in the cloud should also be encrypted, with keys controlled by the data owner. When using services such as AWS or Azure, do not assume encryption will be provided by default. It must be actively requested and driven by the customer organization.

### 3.7. Secure Collaboration and Partner Access

As described in the Supply Chain and Third-Party Oversight section of Passive Measures, third parties present significant risks to IC, and can lead to unauthorized access or exposure if not controlled properly. Third party engagements can take multiple forms, but there are three fundamental control areas companies should address to adequately protect IC across third-party engagement scenarios:

3.7.1. **Centrally Controlled Third Party Access to Company Systems.** Many companies will employ outsourced partners or service providers to manage systems, provide business process outcomes, patent filings, M&A legal support, etc. In some instances, these partners will be accessing systems that contain IC. It is therefore important to deploy standard solutions for this third-party connectivity, which allow monitoring and controls to be applied to limit this access to “need-to-know.” It is often challenging to find the appropriate balance here, as methods such as virtual desktop (VDI) provide more access than required, but are simple and consistent to deploy. Other options include secure VPN or remote application access solutions.

3.7.2. **Secure Collaboration Standard(s).** In many life science business scenarios, organizations collaborate in areas such as drug discovery, pharmaceutical science and diagnostics. This usually involves a collaboration platform where files can be exchanged and/or co-authored and co-edited, with interactive chat capabilities. Regardless of which solution is used, ensure that the contract terms between the collaborating organizations includes provisions on who will administer the collaborative arrangement. It's also important that users have access to training materials, hints/tips on how to secure the content stored in these collaboration tools. Ideally, companies should have a standard partner and service for secure collaboration, so controls for monitoring, access control and transfer restrictions can be consistently enforced.

3.7.3. **Secure File Transfer Standard(s).** Companies should provide tools and mechanisms to securely exchange IC, whether user-to-user, user-to-system, or system-to-system. Often, the user-to-user transfers are built into the secure collaboration tools outlined above. For user-to-system and system-to-system, a different solution is often required. Companies should strive for a standard solution so controls for monitoring, access control and transfer restrictions can be consistently enforced.

**Implementation Guidance**

Data protection tools, processes and controls all require the necessary governance, management and monitoring to properly mitigate risks of IC loss, exposure or theft. They also must all be complemented with strong organizational change management, as many of the controls will require changes in behavior either from users, data owners or both. It is important to focus these change management efforts on the "why," rather than too much on the "what." Users, data owners and business stakeholders will accept an appropriate balance of control and flexibility, if the risk mitigation benefits are clearly explained and demonstrated.

Companies with research labs or manufacturing plants should also plan accordingly when deploying many of these data protection controls. The data movement and business process patterns in these lab and plant sites present unique challenges (e.g., equipment-specific computers, older operating systems, regulatory scrutiny) that should be accounted for proactively. To the extent that any of these or other functions are outsourced or contracted, the organization should also consider emplacing copy/paste restrictions on any remote access systems and modalities to ensure data visible to the contracted entities cannot be copied out of its protected context.

Lastly, DLP systems attempt to manage and control risky behaviors with data. Certain jurisdictions may interpret this monitoring and control as a potential infringement on individual personal privacy. These controls must be clearly positioned and documented as necessary protections for the company and its sensitive digital assets, including IC. Partnerships with the enterprise legal and privacy functions will be necessary to achieve the best outcomes. For some jurisdictions, proactive disclosure to local works councils may also be required to deploy these controls (and organizations would do well to plan for a lengthy review of those disclosures). As stated in the information governance and acceptable use policy statements sections in Passive Measures, it is strongly recommended that companies clearly document within companywide policy that monitoring and controls will be employed to protect company assets.


Figure 3. Active and Passive Measures for IC Protection

## Physical Security Controls

### 4. Physical Security and Human Resource Processes

As introduced in the Passive Measures section, physical security provides a necessary foundation upon which to build and maintain multiple types of access controls. For sensitive information processing and trade secret protection, advisable physical security controls include:

4.1. Limiting physical access to IP/TS processing facilities.

4.2. Periodically reviewing access authorizations for IP/TS processing facilities.

4.3. Employee Proofing/Background Checks, with periodic reinvestigation of privileged roles for large organizations.

4.4. Geofencing smart phone camera use within IP/TS processing facilities or restricting the use of all mobile devices within IC sensitive areas (e.g., manufacturing environments).

4.5. Limiting print usage within facilities and or implementing secure print capabilities.

4.6. Watermarking print to uniquely identify credentials associated with IP/TS processing facility printer output.

4.7. Monitoring employee/contractor activities within the facilities.

4.8. Monitoring for data transfer to/from high risk geographies, supported by a continually updated list of restricted entities.

4.9. All the above is equally applicable to the contingent workforce.

**Implementation Guide**

Conduct a series of red team tests to affirm the physical and logical controls are working in consort to protect IC processing facilities, and systems within which IC is stored, or generated.

## Proactive Analysis

### 5. Centralized Analytics

All of the security controls outlined in the sections above generate activity logs. These logs are comprised of a series of events, alerts and other triggers being monitored or controlled by the individual tool or system. These logs provide a tremendous source of data to indicate overall security posture but are limited to the specific control area for which they are deployed. Companies should build a central analytics capability where the logs and event data from all of these controls can be aggregated and correlated. This provides tremendous value in conducting investigations for security incidents potentially linked to IC loss, exposure or theft. Risk analytics can then be layered onto the system to proactively identify potential indicators of compromise, ideally before the threat to the IC is instigated. Some of the components for this central analytics capability should include:

5.1. Threat Intelligence (discover publicly exposed content).

5.2. User and Device Authentication.

5.3. Data modification monitoring for IC repositories.

5.4. Data Loss Protection:

5.4.1. Endpoint (USB)

5.4.2. Email Monitoring

5.4.3. CASB (web movement)

5.5. Physical Access logging.

5.6. Behavioral Analytics for Insider Threat.

5.7. Data Protection Monitoring.

## Implementation Guidance

Behavioral analytics attempts to establish an accurate baseline of normalcy and alert when any indicators of abnormality are found. Success and positive risk impact in this area have varied but show promise to protect against insider threat. Traditional logging and analytics tend not to readily identify insider abuse as such insiders use access rights mostly seen as legitimate to extract or exfiltrate sensitive data.

Like some of the data protection controls outlined above (e.g., DLP) behavioral analytics may similarly be viewed by some as a potential infringement on individual personal privacy. The same recommendations apply here: Clearly position these analytics controls as protecting the company and its sensitive digital assets, including IC, and work closely with the enterprise legal and privacy functions to ensure the best outcome. Proactively disclose plans to local works councils before deploying these capabilities. Clearly document within companywide policy that monitoring and controls will be employed to protect company assets, and periodically audit use of these tools to ensure maximum transparency on use.

## Conclusion

The time has come for a unified national strategy to defend innovation capital; one which aligns public and private interests, reduces barriers to learnings from prior failures, and shifts the national defense posture from primarily legal courses of action, towards more active, and aggressive forms of curation and protection.

While we look forward to the inevitable and necessary dialogue that must come from a meaningful analysis of these issues and recommendations, without addressing the parochial interests that strangle meaningful improvements, it is certain that the current state of affairs will continue to degrade the international competitive edge of the United States in healthcare innovation. For this reason, we call on all healthcare companies, law enforcement agencies, regulators and lawmakers to come together to address these issues.

Cyber controls, particularly when carefully shaped to address the threats identified in this paper, and particularly when calculated to address known and evolving attack vectors, are the most effective tools to prevent and quickly detect loss and attempted appropriation. Only when these active measures are competently paired with traditionally passive protections, national, and international policy making, collaborative engagement with law enforcement, and public/private partnership, can we hope to build the most comprehensive defense possible for an innovation economy, and against the current 'divide and conquer' strategies of its adversaries.

To maximize IC protection, we have recommended every affected healthcare organization establish a *focused* innovation capital protection program, with a five (5) pronged approach:

1. Continuous identification of IC.
2. Assignment (and periodic update) of the estimated value and ownership of IC.
3. Establishment of comprehensive control and adherence/compliance requirements for IC.
4. Emplacement of active and passive protective controls to close perceptible gaps (as outlined in the control recommendations).
5. Periodic, focused review and sustainment efforts.

While we understand the interests of protecting ongoing investigation sources and methods, and appreciate that certain investigative details must continuously be protected, we believe a

balance must be struck to more robustly activate private industry protection, and further strike at the heart of 'divide and conquer' strategies. To bolster IC protection and information sharing, we therefore recommend that safe harbor allowances be explored to reduce barriers to organizations for sharing early, those causes, conditions and fact envelopes associated with IC loss experiences.

Finally, while we cannot directly recommend change to law enforcement staffing as we did not study this issue directly, it would seem intuitive that an increase in federal law enforcement staffing to target this issue might correlate with improved identification, IC theft prosecution outcomes, and the advancement of the public private information sharing.

## Annex: Works Cited

Bennett, C. (2015, August 11). *Feds charge hackers in massive insider trading scheme*. Retrieved from The Hill: https://thehill.com/policy/cybersecurity/250812-feds-to-charge-hackers-in-massive-insider-trading-scheme

Brachmann, S. (2018, July 27). *Reports Shows Significant Increase in Trade Secret Litigation Since Passage of DTSA.* Retrieved from IPWatchDog: https://www.ipwatchdog.com/2018/07/27/reports-increase-trade-secret-litigation-dtsa/id=99646/

Casey, B. (2012, August). *The Impact of Intellectual Property Theft on the Economy*. Retrieved from United States Congress Joint Economic Committee: https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf

Clapper, J. R. (2016, Feb 9). *Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee.* Retrieved from DNI.Gov: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Donohue, T. J. (2014, November 17). *Intellectual Property Has Huge Impact on Society*. Retrieved from U.S. Chamber of Commerce: https://www.uschamber.com/above-the-fold/intellectual-property-has-huge-impact-society

Fenwick & West, LLP. (2001). *Trade Secret Protection: A Primer and Desk Reference for Managers and In House Counsel.* Retrieved from Fenwick.com: https://www.fenwick.com/FenwickDocuments/Trade_Secrets_Protection.pdf

Getty, J. (2018, February 14). *Three Lessons from the Conviction of Sinovel Wind Group for Trade Secret Theft*. Retrieved from Duanne Morris Green IP: https://blogs.duanemorris.com/greenip/2018/02/14/three-lessons-from-the-conviction-of-sinovel-wind-group-for-trade-secret-theft/

HIPAA Journal. (2015, June 24). *What are the Penalties for HIPAA Violations?* Retrieved from hipaajournal.com: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

International Bar Association. (2018, June 27). *Keeping it secret: the Trade Secrets Directive (citing European Union Directive 2016/943).* Retrieved from International Bar Association: https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=a5a6a6fd-edf6-4b1a-961c-3064a219d0ae

IP Commission. (2019, February). *IP Commission 2019 Review: Progress and Updated Recommendations.* Retrieved from IPCommission.org: http://www.ipcommission.org/report/ip_commission_2019_review_of_progress_and_updated_recommendations.pdf

Legal Information Institute. (2019). *U.S. Code § 1839.Definitions*. Retrieved from Cornell Law School: https://www.law.cornell.edu/uscode/text/18/1839

MAURIELLO, R. L. (2014, May 19). Five Chinese officials indicted for hacking Pittsburgh-area businesses. *Pittsburgh Post-Gazette*.

Office of the United States Trade Representative. (2018). *2018 Special 301 Report*. Retrieved from Office of the United States Trade Representative: https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf

Parrish, W. C. (2018, Feb 23). *In brief US2018-07: SEC issues interpretive guidance on cybersecurity disclosures*. Retrieved Aug 2019, from pwc.com: https://www.pwc.com/us/en/cfodirect/assets/pdf/in-brief/in-brief-us2018-07-sec-cybersecurity-risk-disclosures.pdf

The National Bureau of Asian Research. (2017). *Update to the IP Commission Report*. Retrieved from The IP Commission: http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Toren, P. (2016, May 24). *Definition of a 'Trade Secret' Under the DTSA"* . Retrieved from IPWatchDog: https://www.ipwatchdog.com/2016/05/24/defintion-trade-secret-dtsa/id=69262/

U.S. Department of Justice. (2013). Retrieved from https://www.courtlistener.com/recap/gov.uscourts.wiwd.33833.25.0.pdf

U.S. Department of Justice. (2013, June 5). *Former Engineer For Global Medical Technology Corporation Charged With Stealing Trade Secrets From New Jersey Employer*. Retrieved from https://www.justice.gov/usao-nj/pr/former-engineer-global-medical-technology-corporation-charged-stealing-trade-secrets-new

U.S. Department of Justice. (2018, December 17). Retrieved from https://www.justice.gov/opa/press-release/file/1121706/download

U.S. Department of Justice. (2018, July 6). *Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets*. Retrieved from https://www.justice.gov/usao-wdwi/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets

U.S. Department of Justice. (2018, August 31). *Former GlaxoSmithKline Scientist Pleads Guilty to Stealing Trade Secrets to Benefit Chinese Pharmaceutical Company*. Retrieved from https://www.justice.gov/usao-edpa/pr/former-glaxosmithkline-scientist-pleads-guilty-stealing-trade-secrets-benefit-chinese

U.S. Department of Justice. (2018, March 23). *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps*. Retrieved from https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

U.S. Department of Justice. (2018, December 20). *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*. Retrieved from

https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

United States of America v. Hua, 18 Crim 891 (United States District Court Souther District of New York December 17, 2018).

United States of America v. Maniar, SUE/2013R00623 (U.S. District Court of New Jersey 2013).

United States of America v. Rafatnejad, 18 Crim 94 (United States District Court Souther District of New York 2018).

United States of America v. Sinovel Wind Group, o.13 CR 84 BBC (DISTRICT COURT FOR THE WESTERN DISTRICT OF WISCONSIN June 27, 2013).

United States of America v. Xue, CRIMINAL NO. 16- (Eastern District of Pennsylvania 2018).

Unknown. (2014, September 5). *Protection of Trade Secrets: Overview of Current Law and Legislation.* Retrieved from EveryCRSReport.com: https://www.everycrsreport.com/reports/R43714.html

USTR. (2019, April). *2019 Special 301 Report.* Retrieved from USTR.Gov: https://ustr.gov/sites/default/files/2019_Special_301_Report.pdf

Winston & Strawn. (2019, Feb 27). *EU Trade Secrets Directive: What Are "Reasonable Steps"?* Retrieved from Winston and Strawn LLP : https://www.winston.com/en/thought-leadership/eu-trade-secrets-directive-what-are-reasonable-steps.html

World Trade Organization. (2019). *Part II — Standards concerning the availability, scope and use of Intellectual Property Rights*. Retrieved from World Trade Organization: https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm

World Trade Organization. (2019, October 12). *TRIPS : A MORE DETAILED OVERVIEW OF THE TRIPS AGREEMENT.* Retrieved from wto.org: https://www.wto.org/english/tratop_e/trips_e/intel2c_e.htm

Yeh, B. T. (2016, April 22). *Protection of Trade Secrets: Overview of Current Law and Legislation.* Retrieved from Congressional Research Service: https://fas.org/sgp/crs/secrecy/R43714.pdf

# Annex: Definitions

| Term | Definition |
|---|---|
| **Devices** | Computing devices such as servers, desktop PCs, laptops, tablets, and phones. |
| **Account** | Digital representation of an individual (sometimes called a User ID) used to access a Company Information System or online service. |
| **Credentials** | Something provided by a user to prove their identity; could be a password, token, government-issued identification card, etc. Credential strength will increase depending on the risk scenario and trust level required. |
| **Endpoint Protection** | Solutions and services which secure laptops, desktops and portable devices from malicious code and intrusion, and protect the data stored there. |
| **Third Party** | An outside individual or group, under written contract with Company, providing specific services for Company and thereby acting on behalf of Company. |
| **User** | Any Company Personnel authorized to carry out Company business using supplied or approved devices and technology. |
| **Information and Data** | Includes: technical, financial, employee, payroll, computer systems, sales, marketing, advertising, merchandising, product, benefits, customer data, trade secrets, branding, and other information, wherever such information resides (e.g., printed media, computers, networks, storage media, physical storage environments). |
| **Data Classification** | The method by which an organization categorizes its information, associates sensitivity with that information, and labels such information in digital and printed form. Generally, sensitivity levels correlate to the level of risk associated with loss, abuse or misappropriation of the information. |
| **Personal Data** | Any information which relates to an individual or which can be used to identify, locate or contact an individual, either on its own or when combined with other information under Takeda's control. Depending on the applicable laws, Personal Data (sometimes called 'personally identifiable information' or 'PII' in U.S.) may include, for example, an individual's name, email address, postal address, geolocation information, IP address, telephone number, performance evaluations in any media or format, including paper files and electronic records. |

| Term | Definition |
|---|---|
| **Sensitive Personal Data** | A subset of Personal Data that, due to its nature, has been classified by law or policy as deserving additional privacy and security protections. Depending on the applicable laws, Sensitive Personal Data may include, for example:<br>• Government-issued identification numbers.<br>• Individual financial account numbers and details.<br>• Individual health information and medical records, including genetic and biometric data. |
| **Information System** | A discrete, identifiable collection of technology components such as hardware (servers, laptops, network devices, media, etc.) or software (application, database etc.), either managed by Company or third party, which stores, processes, or transmits Company's information and data. Many Company Information Systems are also called Applications. |
| **CASB** | Cloud Access Security Broker; Ensures network traffic between an organization's premise and those in a cloud context comply with company data security policies. CASB provides insight into cloud application operation and use across an enterprise. Among other things, CASB systems detect rogue cloud application use, protect known and authorized cloud applications by masking, encrypting, or preventing data from passing. |
| **DLP** | Data Loss Prevention. DLP is the tools and practices associated with identifying sensitive data using a variety of techniques (including key words, heuristic analysis, exact/reference data match, form matching, etc.) and then applying organizational protection policies to how that data is moved, or modified within, or upon exfiltration from the organizational network and application perimeter. |

| Term | Definition |
|---|---|
| **Business Process Owner** | • Company business leader responsible for the successful implementation of a business process and owns the information and data within that process.<br>• Ensures the appropriate classification and safeguarding of information and data necessary to enable their respective business process(es).<br>• Defines and regularly reviews access restrictions, classifications and safeguards for information and data, in accordance with applicable policies.<br>• Partners closely with System Owner(s) to ensure business process requirements are adequately met and information and data is adequately secured. |
| **System Owner** | • Responsible for the availability, support and maintenance of the underlying Information System(s) that enable business process.<br>• System owners tend to be in IT, and partner closely with Business Process Owner(s) to deliver these systems and ensure the information and data is adequately secured.<br>• Governs the Data Custodians who manage the technology components within the system, ensuring they have the correct tools and capabilities for protecting information and data. |
| **Data Custodian** | • Oversees the functioning of the information systems on which the data resides.<br>• Delivers services in accordance with defined service requirements.<br>• Regularly reports on designated data and information systems. |

# Annex: Notable IC Theft

These in-depth reviews are noted by the case study icon in the table below which contain links to the individual case studies that are located earlier LINK in this document.

Link: **Case Studies**

| Industry | Intellectual Property Theft Examples |
|---|---|
| **Medical Technology**   | A group of people conspired to steal IC from a pharmaceutical company to benefit a competitive company that they founded. The conspirators included two (2) scientists employed at the pharmaceutical company who subsequently pleaded guilty to stealing IC information they had access to as part of their employment.<br><br>Alleged Activity/Indictment Dates: Jan 2012 - Jan 2016<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Medical Technology** | A Chinese scientist was found guilty for conspiring to steal samples of a variety of rice seeds from a biopharmaceutical research facility where he was employed. The seeds were the result of millions of dollars and years of research and have a wide variety of health research applications.<br><br>Alleged Activity/Indictment Dates: Summer 2013 - Feb 2017<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Medical Technology** | A man pleaded guilty for conspiring to steal IC by participating in a long-term plan to steal corn seeds belonging to two US companies.<br><br>Alleged Activity/Indictment Dates: 2007 - Jan 2017<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2016) |
| **Medical Technology** | A former employee pleaded guilty after stealing confidential and proprietary IC from two (2) different medical device companies with research facilities where the defendant worked. The intent was to open a company in China with aid from the Chinese government and use the stolen IC for personal benefit.<br><br>Alleged Activity/Indictment Dates: Jan 2009 – Jan 2019<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2019) |

| Industry | Intellectual Property Theft Examples |
|---|---|
| **Medical Technology**   | A former employee attempted to steal thousands of company files relating to, among other things, a self-administered pen injector prototype from a medical device company.<br><br>Alleged Activity/Indictment Dates: Oct 2012 – June 2013<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2013) |
| **Technology** | Four (4) executives of a computer company were found guilty after attempting to fraudulently obtain more than $10 million worth of IC and then use it to support customers of their employer for personal benefit.<br><br>Alleged Activity/Indictment Dates: 2010 – Aug 2017<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Technology** | A former employee was indicted for theft of IC after allegedly taking a confidential document containing detailed schematics of a circuit board designed to be used in the critical infrastructure of a portion of an autonomous vehicle.<br><br>Alleged Activity/Indictment Dates: Apr 2018 - July 2018<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Technology** | One of the world's largest telecommunications companies attempted to steal IC from a major US wireless telecommunications company and even compensated employees for providing stolen IC. The company even attempted to obstruct justice by producing false reports.<br><br>Alleged Activity/Indictment Dates: 2012 - 2019<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2019) |
| **Defense** | A man was found guilty for intending to convert IC belonging to a defense contractor relating to, among other things, a naval prototype being developed for the U.S. Navy. While exploring the possibility of gaining employment with the defense contractor's strategic partner, he stole thousands of files belonging to his employer.<br><br>Alleged Activity/Indictment Dates: 2011 - 2016<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |

| Industry | Intellectual Property Theft Examples |
|---|---|
| **Technology**   | A Chinese wind turbine manufacturer was found guilty of stealing IC for its own financial gain from a U.S. based energy technologies firm causing financial losses that exceeded $550 million.<br><br>Alleged Activity/Indictment Dates: 2011 - 2016<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Technology** | A man attempted to steal IC regarding turbine technologies belonging to his employer, a US multinational conglomerate based in Boston. This example is particularly alarming due to the evasive effort used by the conspirator. The defendant attempted to mask the IC theft by using steganography, or the practice of concealing a file, message, image, or video within another file, message, image or video, to hide data files in an innocuous looking digital picture of a sunset.<br><br>Alleged Activity/Indictment Dates: Apr 2016 – Apr 2019<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Chemical** | An American and a Chinese national attempted to steal IC relating to formulations for bisphenol-A-Free; BPA-free coatings belonging to multiple owners. One of the defendants was employed by a research organization which had agreements with numerous companies to conduct R&D, testing, and analysis of various BPA-Free technologies<br><br>Alleged Activity/Indictment Dates: Sept 2017 – Feb 2019<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2019) |
| **Chemical** | After accepting employment with a competitor, a former employee stole proprietary information and IC from a chemical company. Many of the files also contained information that was related to company customers who were also customers of the competing firm.<br><br>Alleged Activity/Indictment Dates: Aug 2013 – July 2018<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |

| Industry | Intellectual Property Theft Examples |
|---|---|
| **Chemical** | A man pleaded guilty for attempting to steal IC from his employer, the world's largest producer of sodium cyanide. Meanwhile, he established a side company whose purpose was to solicit Chinese-based investors to build a sodium cyanide plant in Canada – in direct competition with his employer.<br><br>Alleged Activity/Indictment Dates: June 2015 – Sept 2017<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Chemical** | A man was charged with theft of IC after allegedly stealing digital files from a US-based petroleum company by downloading hundreds of files while he worked for the company. The IC related to the manufacture of a "research and development downstream energy market product."<br><br>Alleged Activity/Indictment Dates: Dec 2018<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Financial Services** | A man pleaded guilty to intentionally accessing a mortgage company's protected computer without authorization to steal client information for his own private commercial gain.<br><br>Alleged Activity/Indictment Dates: Oct 2017 - Mar 2019<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2017) |
| **Multiple Industries**<br>  | Two Chinese nationals associated with the Chinese Ministry of State Security's Tianjin State Security Bureau and APT10 conducted global campaigns of computer intrusions targeting IC and confidential business and technological information at Managed Service Providers (MSPs).<br><br>Alleged Activity/Indictment Dates: 2014 - Dec 2018<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |
| **Multiple Industries**<br>  | Nine people were charged with conducting a massive cyber theft campaign on behalf of an Iranian organization. In total, more than 31 terabytes of data and IC was obtained by using stolen account credentials to obtain unauthorized access.<br><br>Alleged Activity/Indictment Dates: 2013 to Mar 2018<br>Reference: **www.justice.gov** (U.S. Department of Justice, 2018) |

# Annex: Information Categories

**Clinical Trials**

Information documenting the methods, processes, results of a clinical trial, and the actions taken within the scope of Good Laboratory Practice (GLP), Good Clinical Practice (GCP), and pre-clinical reporting.

Examples: Study Concept Documents, Clinical Data/Results, Protocols and Protocol Amendments for Phase 0 to 4 Interventional Studies and Non-interventional Studies

**Compliance Information**

Information regarding the status and measures associated with regulatory and legislative monitoring and reporting (State or Local Government related mandates, HIPAA, FDA, SEC, OSHA, EPA).

Examples: Corporate Integrity Agreement information, Government filings, Government audits

**Financial Information**

Information in support of a company's financial system that include the circulation of money, credit and investment related statements, and banking information.

Examples: Financial plans, material non-public financial outcomes, merger and acquisition information and plans.

**General Business**

Business information not generally covered within other categories.

Examples: Meeting minutes, Human Resource information (excluding personal information), Information systems information (excluding protection methods or systems diagrams), Training records

**Innovation Capital**

Information pertaining to exclusive rights to intangible assets, including but not limited to discoveries, inventions, and trade secrets.

Examples: Lab notebooks, manufacturing recipes and processes, designs, impending patent filings, innovations, and design patterns

**Legal**

Information documenting a company's legal transactions, strategies and other records.

Examples: Minutes from Board of Director meetings, legal settlement information, mergers and acquisition information, proprietary or competitive contract information

**Personally Identifiable Information**

Personally Identifiable Information (PII) refers to any data, or combination of data

which might potentially be used to identify a specific individual.

Examples: Name, age, gender, ethnicity, address, social security number, phone number, date of birth, email address, bank account, professional title(s) and affiliations, employee identification, marital status, compensation information, patient identification, clinical trial subject identification information, diagnosis, or treatment information.

**Patient Safety**

Records regarding intake, processing, analysis or disclosure of adverse as required by Good Pharmacovigilance Practices (GPVP).

Examples: Adverse event, analysis, risk communications, and patient safety data

**Product Marketing, Sales and Long Range Plans**

Product promotional data, long range plans, and market positioning product plans.

Examples: Brand plans, marketing plans, material approval and compliance (MAC) documentation, sales and marketing information

**Product Processes and Quality**

Information related to the processes for manufacturing, packaging and distribution used to ensure quality and safety of a company's products and activities required for Good Manufacturing Practice (GMP) and Good Distribution Practice (GDP).

Examples: Batch Records, Analytical Methods, Devices, Therapies, Packaging