InteliSecure

## At a Glance



## Are you addressing your biggest data loss risk?

For many organizations, defining Intellectual Property (IP) isn't a black-and-white call, and the difficulties they have clarifying the substance and value of those assets leaves the business exposed to serious risks. Step out of the gray areas of cloud IP definition and take steps to protect your most critical data assets.

INTELISECURE GUIDE

# Protecting Intellectual Property: Black, White, and Shades of Gray

Around the world, across a variety of industries, organizations have one perplexing thing in common: their data protection programs are focused solely on regulated data such as social security numbers, credit card account information, and other Personally Identifiable Information (PII).

Complying with data privacy regulations is important, but rarely is regulated data the only data worth protecting in a company. In most organizations, losses associated with regulatory fines presents far less risk than the potential losses associated with intellectual property theft—loss of market share, loss of competitive advantage, loss of revenue, and potentially loss of the entire company.

IP theft is among the greatest threats to your business, and it will not likely happen through an external attack. In this guide, you'll learn the consequences of IP theft, why so many organizations struggle to identify and protect IP, and how a data protection program that's focused on critical assets can help you protect even unstructured IP.

## WHY IP IS SO VALUABLE

Today's global economies are built primarily on ideas. When you hear that we are living in the information age or we live in an economy of ideas, what you're really being told is that we no longer build wealth based on the manufacture of physical goods or the possession of commodities or resources, but by creating and marketing *ideas*.

The ideas that are unique inventions or creations critical to a business's operation or differentiation are IP. In the entertainment industry, **copyrighted** works drive the economic engine for their creators. Organizations that build software products or manufacture drugs clearly understand that **patent protection** for their inventions is essential to their business. People in the restaurant business or who trade in chemical formulas understand that **trade secrets** are at the core of their business.

These types of IP are essential to sustaining your competitive advantage.

## WHAT HAPPENS WHEN INTELLECTUAL PROPERTY IS STOLEN?

IP theft is more difficult to identify than the theft of regulated data such as credit card information; those thefts are often discovered when the numbers are sold on the dark web.

In contrast, IP is often stolen for the benefit of an entity that is unaware of the serious nature of the crime. For example, an employee might apply for a job at a competitor claiming they have the skills to build a better product. They get the job and take their former employer's product designs with them to use in building a competing product.

Other times, the entity that receives the stolen property has directly commissioned the theft. One highly publicized instance was the case of American Semiconductor, which lost nearly $1 billion in enterprise value, cut 700 jobs, and nearly went out of business when an employee sold IP to a Chinese partner.

American Semiconductor likely had all the external protections and anti-malware you could ever want, but they lacked proper mechanisms to monitor their data and how their people interacted with it. That oversight nearly cost them their company.

> **"THEIR STRATEGY WAS TO KILL US."**
> — American Semiconductor CEO Daniel McGahn

## WHAT IS YOUR INTELLECTUAL PROPERTY WORTH?

Surprisingly, many organizations don't understand the crucial role—and true value—of their aggregated trademarks, copyrights, and trade secrets in their business success.

- **Could your competitors more effectively compete with your business** if they knew how you sold your products and services and understood your entire strategic plan?

- **If you sell direct to consumers,** how valuable is the ability to establish and convey trust through a trademark?

- **How much does your profitability rely** on your customer lists or the processes you use to deliver services?

All of your perimeter security technologies and your intrusion-prevention systems will not protect you from an attack performed by or leveraging a person who has valid credentials inside your environment. It is vital that you monitor your people and your data. However, most organizations place the majority of their emphasis on protecting data from outsiders. Insider protections are an afterthought. Until we shift this paradigm, attackers will continue to succeed.

## WHAT ARE YOUR LEGAL OPTIONS FOR PROTECTING INTELLECTUAL PROPERTY?

Legal protections help ensure that the inventor of an idea has certain exclusive rights to profit from that idea for a limited time.

**Patents** offer a strong level of protection to a product or process, guaranteeing exclusivity for the patent holder for a limited time. Patented information is not secret. However, in the period before the patent is filed, designs for inventions are extremely sensitive.

**Copyrights** grant the holder specific, exclusive rights for a long period of time. Copyrights are generally assigned to creative works such as books, music, and films and to business assets such as websites, marketing material, and slide presentations.

**Trademarks** offer extended, renewable protection to the holder. The value of a trademark is in the protection it gives the owner for preventing someone else from using the term, idea, or work.

**Trade secrets** are protected only as long as they remain secret. Trade secrets are among the most common, most valuable, and least understood types of intellectual property—and are the most vulnerable. The term "trade secret" covers a wide range of intangible assets from product formulas and recipes, to training methodologies, know how, industrial design, and business processes. It is difficult to defend your trade secrets if you have not clearly defined what they are.

## WHY ARE WE NOT PROTECTING WHAT'S MOST IMPORTANT? IT'S COMPLICATED.

Protecting IP requires making calls that are not black and white, yes or no. This type of data is often unstructured and doesn't fit neatly into established categories like regulated data does. It takes information security teams into gray areas that are uncomfortable. Before you can protect your IP effectively, you need to identify the difficulties around dealing with those gray areas.

Here are some of the most common issues.

### It's difficult to define IP

It's true that protecting IP is not as straightforward as protecting other types of sensitive information. Regulated information is well defined in the public space. Something is either a credit card number or it's not. It's either PII as defined by global regulations or it's not.

Mature organizations have a list of people who can handle that regulated sensitive information and have defined acceptable use of that information. The information security team can set up rules to enforce those documented policies easily. It's black and white.

IP protection, in contrast, is messy. It isn't black and white. It's one big squishy gray area. Although a few rules govern how IP cases can be brought to court, no external entity dictates what constitutes IP or how an organization must protect it.

IP is difficult to define even for the organizations it belongs to. To properly protect IP, the information security team must engage the business leaders who create and profit from it. They need to know what drives revenue for the organization, what role the IP plays in that revenue, and whether the information would be valuable to an outside entity. And they need to understand who plays a role in the creation, storage, usage, and transmission of the data.

After that, they need to speak with the legal team to see what portions of the IP are legally protected and therefore not sensitive—and what portions of the IP are considered trade secrets or know-how and have few legal protections.

### It's difficult to quantify the risks associated with IP

Even when IP is defined, quantifying the risk of its loss is a challenge. The ability to quantify risk is a measure of a company's overall health. Publicly traded companies must produce an annual report known as a 10-K report. In that report, section 1A is a detailed list of the risk factors affecting their business.

In that evaluation, regulatory fines are risks that are easy to understand. If you don't comply with a specific regulation, the regulating body will fine your company for non-compliance with data security regulations. The company can look at the legal precedent to see what organizations were held accountable and what the actual costs were in the event of a breach. It's black and white. And it's easy to quantify the value of mitigating that risk too: *I am going to invest X dollars to reduce my exposure to a risk of a fine that will cost Y dollars.*

Not coincidentally, effectively protecting IP will also mitigate a significant number of those easily quantifiable risks. However, organizations struggle to quantify risks associated with not protecting the IP itself, even though those risks are very real. It's a gray area.

## It's difficult to define the rules related to IP

Organizations often maintain lists of users who can interact with regulated information. Data security regulations also typically define the allowed activities related to that information. For example, the Health Insurance Portability and Accountability Act (HIPAA) states that a health record being transmitted via email must be encrypted. That rule is black and white—easy to implement and enforce.

For information security teams asking whether a user can interact with IP inside an organization, the answer is almost never yes or no. In nearly all cases, it depends.

That answer is governed by a variety of factors related to the person's job role and normal pattern of behavior. How that information should be used often changes quickly, and the changes are typically not well defined. The entire rule set for IP is a gray area.

## It's difficult to coordinate communication about IP

These are conversations that many organizations' Information Security teams are unwilling or unable to engage in.

In many organizations, data protection programs are categorized under the same umbrella as information security tools. This makes sense from an outside perspective; after all, data protection programs do fall under information security and are often operated under the same budgets as traditional security technologies such Security Incident and Event Management (SIEM), Endpoint Protection Platforms (EPP), and Intrusion Detection and Prevention Systems (IDS/IPS).

**Data protection programs though, are fundamentally different from those technology tools because they require business engagement in order to be effective. And that can be a challenge.**

Even in organizations that attempt to force that communication to happen, most information security teams do not use the same language (or jargon) to communicate security concepts that business leaders use. Business leaders are becoming more technically savvy, but many information security teams struggle to provide information in ways that make sense to their executive teams.

As a result, the information security teams default to the areas where they are most comfortable: protecting regulated data—with black-and-white security tools. A firewall checks a list of senders, destinations, and ports and allows or denies each piece of traffic that attempts to traverse its network segment. A web gateway puts websites into categories and allows or denies users access to that category. A traditional antivirus program scans a file against a list of known bad files and if a match is identified, the program blocks or quarantines the file.

This is all very straightforward and not nuanced. The decision is black and white.

## OPERATING IN THE GRAY AREA: LOOKING TO THE FUTURE OF IP PROTECTION

There is good news for companies that recognize the value of their IP. Emerging and newly available technologies are helping companies overcome the difficulty of working in the gray areas of data protection. Artificial Intelligence (AI) and machine learning are areas showing tremendous promise. Although automated technologies aren't capable of supporting nuanced decision patterns, they can help streamline responses, improve reporting, and allow for dynamic actions.

**AI is an exciting concept and a major leap forward. It is also not a silver bullet. Organizations still must engage with the business to define what sensitive IP is, and they should start doing that now.**

Fortunately, managed data protection solutions are enabling companies to access highly specific protections for structured and unstructured data while dramatically reducing the complexity of security management for their staffs.

Unlike broad, non-specific managed security services, managed data protection services focus specifically on protecting critical data assets, including both regulated data and the diverse, unique, and often unstructured data that gives a business its marketable advantages.

A professional managed data protection provider starts by identifying those critical data assets, then:

- Selects and implements technology solutions
- Creates proven security policies to ensure compliance and strong protections
- Aligns with user and business needs to balance protections within business operations
- Continually evaluates and refines the program to keep up with the continually shifting security landscape

Capabilities exist to protect sensitive IP, and the stakes are higher than they've ever been. The question is not whether you can afford to protect your IP. The question is quickly becoming whether you can afford not to.

## LOOKING FOR A PROVEN APPROACH TO PROTECT YOUR INTELLECTUAL PROPERTY?

InteliSecure offers consulting services to help organizations navigate the gray areas of critical asset protection. Contact us to start working through your complex data protection conversations—and find the solution that fits.

## ABOUT INTELISECURE

InteliSecure specializes in making data protection easy, fast, and cost-effective for companies of nearly every size. More than 500 clients with over 2 million managed users rely on our services and specialists to protect the integrity and safety of their sensitive information. With more than 15 years' experience and partnerships with some of the world's biggest names in cyber defense, we make data security and compliance easy by providing effective data protection at a lower cost, eliminating the strain on IT organizations and reducing the risk of confidential information getting into the wrong hands. Unlike other security providers, we focus on business outcomes—providing data and reports that make sense to business and security executives alike. InteliSecure serves clients globally with security operations centers in the United States and the United Kingdom.

InteliSecure sales@intelisecure.com | www.intelisecure.com

**5613 DTC Parkway, Suite 1250 Greenwood Village, CO 80111 | + 1 (720) 227-0990**
**1 Lindenwood, Chineham Business Park Crockford Lane, Basingstoke, RG24 8QY, UK | +44 118 976 8960**