Leading Authority Doug Kaminski On 3 Key Ways To Protect Your IP

#FearlessLaw
on
High
Performance
Counsel

HIGH PERFORMANCE COUNSEL

The development of the Internet of Things has allowed businesses across the globe to expand in new and exciting ways. We can share our thoughts, ideas, and even secrets, freely across channels, servers and file shares. This type of total-freedom also disinhibits nefarious third-parties, intent on stealing what you have, what you know, and what you care about the most. According to a 2017 PwC survey of 10,000 executives, 45% of respondents at companies that had a cyber incident reported that stolen intellectual property had a direct impact on their business – a significant increase over previous years. Whether that's trade secrets, industrial designs, credit card info or proprietary data, the threat of having your Intellectual Property stolen is very real and should be a cause of concern for any business leader. It does damage to both your bottom line and your reputation.

In the e-discovery field, handling sensitive and sometimes classified client data is an inherent part of the business. Security threats regarding this data are more nuanced and more sophisticated than ever before. Internally, you need to be aware of things like malicious insiders or if an ex-employee goes rogue and takes your IP to a competitor. Externally, you need to be aware of the ever-present threats of phishing, malware, and foreign state actors that can bring down your servers, jeopardizing the IP of your business and your client's business.

It takes a village, and an entire e-discovery toolkit, to employ secure information governance policies that protects your IP. Here are three key steps to mitigate risk when it comes to guarding your Intellectual Property:

1. Maintain and Monitor Internal Access

One of the hardest things to control is the sharing and leaking of data and IP from internal employees. It's hard to manage and even harder to identify. One way to mitigate this internal risk is to classify data by its sensitivity and value, and segment access to important data based on the employee type and if they need this data to perform their jobs. Another way to manage the amount of data shared between employees is to have your IT team actively monitor and regulate the file sharing platforms used internally. This type of proactive approach helps stop problems before they start.

2. Classify and Delete Your Data

The easiest way to limit the damage of data leaks is to control and limit the amount of sensitive data that is readily available to employees and external parties. You can use things like analytics and technology assisted review to redact and delete unnecessary files and archive data that you may need later. To gain a topline view of what might be at risk and to what employees, you can also use cluster visualization and email threading capabilities to identify IP terms that might be at risk via a simple keyword search. These types of proactive actions help limit what can be exposed by malicious third-parties or insiders, saving you time and stress.

3. Finetune Your Response Plan

It's very hard to recover when you've lost your intellectual property, but if you do, it's important that you have a coherent and concrete crisis plan in place to limit damage. The origin of your crisis plan should take place well before an actual crisis happens. This means gaining alignment with your key internal stakeholders, building an insider threat response program, and holding regular crisis trainings to ensure that everyone is internally aligned with your plan of action if, and when, your IP is leaked externally. This crisis plan should continuously evolve as the world of cybercrime changes; a third-party assessment on the potential weaknesses in your data security also helps.

It's a wild world out there. Hopefully these few pointers help in the never-ending battle of information security.

Doug Kaminski serves as director of major accounts for Relativity. In his 20+ years in the legal industry, Doug has consulted with some of the world's most highly regulated companies, including many Fortune 100 companies, to help them gain control of their data and tackle their unique challenges surrounding e-discovery and information governance. Prior to joining Relativity, Doug served as senior director of information governance at Huron Consulting Group (now Consilio) and held positions at Symantec, Clearwell Systems, Wolters Kluwer, and LexisNexis Document Solutions.

Welcome to

HIGH PERFORMANCE COUNSEL

High Performance Counsel provides a valuable sounding board for legal sector leadership on the issues and opportunities facing the legal sector in the next decade. We call on a diverse spectrum of thought-leaders to share their perspective on what works, what doesn't and where it's all headed. Join us.

Learn more