Buchanan Ingersoll & Rooney PC

Cybersecurity & Trade Secret Audit

A Multidimensional Approach to Protecting Your Business

Protecting your confidential information means guarding the very core of your business. Your success and reputation depend, in part, on your ability to protect your own confidential information and trade secrets, as well as those of your trusted customers, partners, suppliers, and service providers.

How We Can Help You

Conduct a Trade Secret Audit

Have you put in place the necessary procedures and protocols to protect your business from the misappropriation of your confidential information? Many businesses – including some of the largest global companies – fail to do so. And courts today are notoriously unsympathetic, should a breach occur, when the right protections have not been in place. You can look to our team of Cybersecurity, Intellectual Property, and Employment attorneys to proactively conduct a thorough Trade Secret Audit before you suffer a loss. Protecting yourself with a comprehensive audit may be the proverbial "ounce of prevention" worth more than the "pound of cure."

What is a Trade Secret Audit?

Our team is ready to work with your internal specialists to assess how well your enterprise's confidential business and technical information are currently being secured against cyber attacks and misappropriation. We can conduct a comprehensive audit of your current data security processes to identify both strengths and weaknesses, and prioritize the steps needed to fix vulnerabilities. After an attack or theft occurs, it's too late. While some may not want to spend the time or money for such an audit, complacency can be far more costly.

What Information Needs Protecting?

Do you have trade secrets, such as technical information, that would cause major damage to your company if shared with a competitor? How about confidential customer information? Perhaps it's your financial data, the buying patterns of your customers, or even information about businesses and people with whom you have relationships. It's not always about formulas and secret recipes. The information that resides in every corner of your business has value for those who may wish to do your business harm.

WE WORK WITH CLIENTS ACROSS MULTIPLE SECTORS

County and Local Governments and Agencies • Educational Institutions
Emergency Medical Services • Energy and Public Utility Companies • Financial Institutions
Government Entities • Healthcare Providers • Hospitality Industry • Insurance Companies
Liquidation Services • Manufacturers • Retailers • Security Alarm Companies
Software and IT Companies • And More

We Ask the Right Questions

We ask the necessary questions to assess your needs and build a customized plan to get you prepared. There are several questions that you should consider:

- If your company's trade secrets have been targeted by existing or former employees, competitors, or hackers, would you be aware of it?
- If you've had minor breaches, where have they come from — employees (current or former), consultants, suppliers, competitors, or any other parties?
- How effective are your internal information technology security practices and forensic abilities in determining whether your trade secrets are secure?
- What training do you provide your employees on their responsibilities for protecting trade secrets and the actions they should take if they suspect something?
- Does your company have someone who is responsible for granting employee access to trade secret information?
- What is the legal review process used to determine whether something is a trade secret?
- Do you have a security checklist for periodic internal audits?
- Do you review the security protocols of your outside accounting and law firms, especially when they have been entrusted with your confidential business and technical information?
- When approaching a merger, acquisition, or potential deal involving external financial organizations, consultants and others, do you factor in potential points of information theft?

A Three-Pronged Approach to Your Protection

Intellectual Property. Our IP team plays a key role because they know technology inside and out. They can work with your in-house counsel to provide guidance on establishing and implementing protocols of trade secret protection.

Employment. You also need to consider the causes and sources of misappropriated information. A common source is employees who are leaving the company. Perhaps they are upset and simply want to do you harm. Or perhaps they download your information to start their own company or use your information as leverage in the job market. We know how to draft employment contracts, non-compete agreements, and non-disclosure agreements that have teeth. If you must go to court to prevent disclosure or respond to an incident, you will need to prove these precautions have already been in place.

Cybersecurity. Our cybersecurity team will examine the policies and practices you have in place, assess any gaps, and recommend steps to strengthen your security program. Any hack and misappropriation of data can have disastrous financial and reputational consequences. We can also bring in a forensic expert to take an independent look at technical systems. We can help keep you from becoming a cybersecurity statistic.

Marc S. Adler | Of Counsel, Intellectual Property | marc.adler@bipc.com | 212.440.4468

Sue C. Friedberg | Shareholder, Cybersecurity & Data Protection | sue.friedberg@bipc.com | 412.562.8436

Jaime S. Tuite | Shareholder, Labor & Employment | jaime.tuite@bipc.com | 412.562.8419