

27-Point IP Security Self-Questionnaire

Use Cerulean's free self-assessment to help you begin to identify gaps in your trade secret and intellectual property security.

Cerulean provides a more formal, one to two-day diagnostic service for executives and small business owners. Clients receive a formal analysis and set of prioritized recommendations including (where information exists) estimated costs and timelines. Clients can then use Cerulean's report to close these gaps themselves or draw upon the report to issue a request for proposal (RFP) to bring in outside help. If you'd like more information on this confidential diagnostic service or other intellectual property security expert services, please contact our Managing Director at +1.757.645.2864 or send an email to info@ceruleanllc.com.

Copyright 2008-2010 Cerulean Associates LLC. All rights reserved in all countries. Reproduction is not permitted without prior authorization.

This is not a legally-binding assessment tool or set of recommendations. Information and questions in this document draw on a variety of sources, including published reports, interviews and research, which may or may not have been prepared or conducted by Cerulean Associates LLC. Cerulean Associates LLC does not warranty the accuracy of the information or the questions contained in this document. The contents of this publication are intended for general information only and should not be construed as legal advice or a legal opinion on specific facts and circumstances. Cerulean Associates LLC assumes no liability for actions taken or not taken as a result of the information in this document. Send questions or concerns to: Managing Director, Cerulean Associates LLC, PO Box 498, Williamsburg, VA 23187-0498 US.

Instructions

Answer each question below to the best of your knowledge. If you are not sure, chances are you should mark “No.” Do not mark “Yes” unless you have some level of documented proof (e.g., training schedules, policies in hand, etc.). This is the time to be critically honest.

There are 27 questions. At the end of the self-assessment is a rating scale.

#	Question	Response
1.	Do you hold annual reviews with your legal counsel and management team to discuss the legal intellectual property and trade secret protections available to you (including the status of private customer information)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.	Does your legal counsel review all documents and other information to be made available outside your company to ensure trade secrets and newly discovered intellectual property are not inadvertently published?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.	Has your legal counsel crafted an intellectual property (IP) / trade secret primer for all personnel?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.	Do you hold yearly training or refresher reviews on IP and trade secret basics?	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.	Do you review with employees your company’s ownership rights in IP and trade secrets invented by your employees?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.	Do you review your company’s ownership rights in any jointly developed intellectual property and trade secrets with contractors, consultants and outsourced groups working for your company?	<input type="checkbox"/> Yes <input type="checkbox"/> No
7.	Does your firm have a formal intellectual property and trade secret security policy in place endorsed by senior management?	<input type="checkbox"/> Yes <input type="checkbox"/> No
8.	Are intellectual property and trade secret security policies regularly audited?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9.	Do you have a cross-functional team responsible for advising management on IP security controls and risks?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.	Does your company review new product-related documents and presentations for appropriate disclosures and confidentiality notices?	<input type="checkbox"/> Yes <input type="checkbox"/> No
11.	Does your company review new process-related documents and presentations for appropriate disclosures and confidentiality notices?	<input type="checkbox"/> Yes <input type="checkbox"/> No
12.	Is copyrighted material controlled with formal review and authorization?	<input type="checkbox"/> Yes <input type="checkbox"/> No
13.	Do you regularly inventory and track all intellectual property information (such as drawings, formulations, and so forth)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
14.	Do you regularly inventory and track all trade secret information (such as secret process flow diagrams and details)?	<input type="checkbox"/> Yes <input type="checkbox"/> No

#	Question	Response
15.	Do you have controls in place to prevent any one individual – such as a computer department (IT/ICT) employee or contractor – from being able to steal your intellectual property or trade secret information without being detected?	<input type="checkbox"/> Yes <input type="checkbox"/> No
16.	Are the computer backups of your information encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
17.	Does your computer department take a “snapshot” backup of the data and emails of any employee or contractor who will be leaving your company?	<input type="checkbox"/> Yes <input type="checkbox"/> No
18.	Do your product development agreements (or JDAs) include clarification of who is responsible for identifying potential new intellectual property or trade secrets?	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.	Do your standard operating procedures (SOPs) or work instructions (WIs) include specific steps someone could use to duplicate your intellectual property or a secret process?	<input type="checkbox"/> Yes <input type="checkbox"/> No
20.	Is there a physical-based access system (keys, badges, etc.) to get into your company offices?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21.	Are visitors to your company offices required to sign-in with specific information such as who they are there to see?	<input type="checkbox"/> Yes <input type="checkbox"/> No
22.	Is there a computer-based access system (userID and password, biometrics, etc.) to get into your company’s computers and network?	<input type="checkbox"/> Yes <input type="checkbox"/> No
23.	Are there security policies and training for personnel who telecommute or travel frequently?	<input type="checkbox"/> Yes <input type="checkbox"/> No
24.	Are your frequent travelers (such as sales personnel) regularly trained on how to safely use hotel business centers and dispose of confidential information while on the road?	<input type="checkbox"/> Yes <input type="checkbox"/> No
25.	Do personnel with access to confidential and private data undergo some level of vetting / background checks prior to access being granted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
26.	Do you have a “clear desk” policy for sensitive or confidential information that is actually enforced?	<input type="checkbox"/> Yes <input type="checkbox"/> No
27.	<i>For US companies only.</i> Are personnel, vendors and customers reviewed for Bureau of Industry & Security (BIS) red-flags?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Scoring

Count the total number of questions that you answered “No” and compare to the chart below.

Note: if you outsource some of your company’s work to people or companies in countries identified by the US government as having poor intellectual property controls, multiply your total “No” count by 1.25. For a current list of such nations, download the most recent “Special 301” report: www.ustr.gov

# of NO's	Consequences
26 or more	<i>Fiasco.</i> It may be too late. Some of your intellectual property or trade secrets have probably left your hands.
19-25	<i>Critical risk.</i> Your intellectual property and trade secrets can be stolen easily without your knowledge. Get help now.
7-18	<i>High risk.</i> Historically, this is the range of most companies who suffer intellectual property and trade secret theft. Without significant improvement, you should expect at least some of your confidential information and competitive ideas to be stolen.
3-6	<i>Low-Moderate risk.</i> Good work. Use the questions in this self-assessment to guide your future improvements. Consider bringing in an outside expert to conduct a workshop tailored to your needs to help define and jumpstart reasonable improvements.
2 or less	<i>Congratulations!</i> You are on your way to best-in-class corporate espionage protection in the globalized economy. Take a look at our “other areas to consider” below for ideas on where to assess next for possible gaps and opportunities for improvement.

Other areas to consider: documenting the technical evolution of new products and services (stage gates, design control, quality by design, etc.), your vendor/supplier selection and qualification program, control of computers, proper email and internet usage audits, laboratory controls, electronic data integrity, financial controls, internal computer network alerts, regular computer security reviews, and so on.

To implement a practical corporate espionage program in-line with your new medicinal product development efforts, consider reading and adapting suggestions from the chapter, *Protecting Your Intellectual Property from the Inside Out*, in the book [Best Practices for Biotechnology Business Development](#).