Designing a high-performance brand protection solution

Kodak

Executive summary

In today's global marketplace, companies are in a perpetual race to protect their brands from attackers who seek to capitalize on successfully created reputations. Brand attacks come in a variety of forms, such as counterfeiting, gray market, black market, tampering, compatibles, copyright, trademark, and patent infringement. Despite their efforts, several companies are falling behind as criminals continue to find and refine their methods for committing fraud. This white paper focuses on product protection measures affecting brand reputation. Specifically, issues pertaining to solution architecture, business challenges, and counterfeit risks are addressed.

Initially, it might seem counter-intuitive that criminals with limited resources and crude technologies are repeatedly outwitting multi-million dollar brands. However, the reality is that many of today's attackers are not "mom-and-pop" shops but sophisticated businesses, operating globally. Today's criminals are well-funded and can easily purchase the knowledge or tools they need to commit fraud. In addition, factors such as supply chain complexity, outsourcing, lack of monitoring, limited awareness or failure to implement basic security solutions all contribute to a brand's vulnerability.

The key to closing this widening gap is to design a comprehensive brand protection solution that utilizes both offensive and defensive strategies, in order to create a tightly integrated end-to-end system. Creating such a comprehensive solution requires a multi-phased approach:

- **Assess** the current state including brand vulnerabilities and needs
- **Design** the future state
- **Protect** by implementing the appropriate technology and process solutions
- **Monitor** the brand for successes and emerging threats
- **Enforce** through investigations, civil actions, and legal actions

Moreover, when designing such a solution, the optimal strategy should be built using five key brand protection building blocks — governance and policies, process, technology, infrastructure, and people. Once such a comprehensive solution has been developed, a brand owner can be confident that the pieces will work well together, rather than relying on a chaotic patchwork of different technologies and approaches.

There are several benefits of following such a disciplined methodology, including the ability for companies to protect their pricing, margins, market share and revenue base, while thwarting off threats to their brands, trademarks, copyrighted material, patents, and intellectual property rights. Designing a high performance brand protection solution is a necessity for any organization that is serious about its brand reputation.

Business Challenges

Counterfeiting is a large and growing problem affecting almost every industry. Estimates for the percentage of world trade that is counterfeit range from 2% to 8%. US Customs and Border Protection (CBP) reports that they seized $1.7 billion worth of goods in 2013 that violated intellectual property rights[1]. Counterfeiting is currently estimated to cost the global economy $1 trillion annually. Other estimates say that the projected value of global trade in counterfeit and pirated goods will be $1.7 trillion by 2015[2]. Add to this the costs of product diversion which directly cost companies $1.4 billion in wasted channel incentives alone[3]. However, current spending by firms to combat these losses as a percentage of related global financial losses is less than 1%[4]. For a problem that's been around for decades, what causes such a wide disconnect? We believe there are seven key reasons that explain the discrepancy.

Maintaining brand security is a complex and amorphous problem.

1. Maintaining brand security is a complex and amorphous problem, which requires an intricate set of solutions. A different solution set is required, depending on the problem (e.g., diversion or counterfeiting) and the circumstances unique to each brand and market. In the case of counterfeiting, fraudulent products range from mundane products like socks and coffee beans, to high-end machines such as Rolls Royce aircraft engine parts and Ferrari internal finishings. Moreover as the problem changes with time, so must the solution. For example, using an antiquated single layered hologram technology to protect an expensive life saving drug is a recipe for disaster.

2. "Brand ownership" is not always clear. There is often limited understanding of who is responsible for brand security, who needs to "budget" for the security, and how individual brand protection schemes support overall company goals. It is often the case that solutions are ad hoc, reactive and localized. This is especially true in companies where there is no centralized office of brand protection. When there is no single person or department in charge of the problem, solutions tend to be reactive and thereby fail to address the entire scope of the problem.

3. There is very often an unclear definition of the problem. Are the products being exploited due to limited protection, ineffective policies, pricing differentials, supply chain tardiness, infrastructure shortcomings, etc.? Without an accurate definition of the scope or goal, it is impossible to make progress.

4. Companies may consider brand protection as an added cost of doing business rather than as an investment to maximize profitability (or minimize revenue loss). While on the surface it may seem to be merely a different way of looking at the same cost, in reality it is a major organizational shift. When a company thinks of brand protection in the same category as marketing, it has truly made the leap forward from being reactive to proactive about their security. As one would imagine, a reactive approach often leads to an ineffective and rudimentary system, while a proactive approach sets the stage for a world class system.

5. The cost of inaction is often perceived as low. Since most companies don't quantify the cost of a potential liability or the opportunity cost associated with lost sales, they tend to ignore it altogether. This is probably because return on investment (ROI) calculations can be difficult. For example, how does a brand calculate liability estimates when the liability constraints are not clear? How does an organization estimate revenue loss due to counterfeits when it doesn't know the scope of the problem?

6. Choosing among the various technologies and vendors in the market place is a tedious, time-consuming and complex process. Which technology is best suited to both track diversion and to prove authenticity on a perfume bottle? What will stand up to the scrutiny of diverters but be economical to apply on a packaging line? How does one evaluate the efficacy of different brand protection solutions? Who is the right partner? Is it a security integrator, security consultant, service provider or technical solution provider?

The challenge is matching the right technology and the right partner with the appropriate business needs and constraints.

1. U.S. Department of Homeland Security, Intellectual Property Rights Seizures Statistics, Fiscal Year 2013 (2014). http://www.cbp.gov/sites/default/files/documents/2013%20IPR%20Stats.pdf
2. International Chamber of Commerce / BASCAP, Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy (2011).
3. Deloitte and the Alliance for Gray Market and Counterfeit Abatement, "When Channel Incentives Backfire", 2011
4. Vandagraf International, "Anti Counterfeit, Brand Protection & Tamper Evident Solutions," November 2013

7. Insight by any one party into the extent of the overall problem is limited. Many successful brands have not fully examined their vulnerabilities or established baselines. Additionally, many companies are reluctant to share their data with others for fear of revealing problems that may adversely impact their reputations. Further, there has been no "one way" or agreement on measuring counterfeiting losses, so it becomes difficult to compare brand protection issues and strategies across companies in the same industry, let alone across industries. This is one of the leading contributors to inaction. When contrasting this with the counterfeiters, criminals are willingly sharing all kinds of information, exploits and "best practices" openly and transparently across various channels.

Truly, it is no surprise that the good guys are falling behind.

Let's step through each of these phases to get a better understanding of the critical components.

Assess: This first step involves identifying and prioritizing key problems. These include issues such as extent of the problem, consumer capabilities, distributor capabilities, sources of counterfeit entry, risks, etc.

A large part of the assessment phase is spent identifying the most pressing business needs, and identifying quick wins to begin to turn the tide of the war. In this phase, it is also important to assess current brand protection activities already in place in the company, including those not formally labeled as brand protection. During the assessment phase, the project team is focused on dividing the problem into manageable chunks, prioritizing issues, and gaining consensus on the true scope of the problem.

The Optimal Solution

On the surface, it may seem futile to create a complete brand security solution while well-funded adversaries are standing on the front porch — yet there is still hope. More and more brand owners are being proactive and recognizing that if they are the "last adopter," they are the easiest target for counterfeiters. Early preparation and collaboration with solution providers greatly increases a company's odds of overcoming attacks on their brand. More and more companies are seeking partnerships with solution providers to provide complementary and integrated brand protection solutions. As these collaborative approaches drive the development of better solutions, the war can still be won.

Designing an end-to-end solution is a prerequisite for establishing a tightly integrated and a secure brand. To make the vision of a secure brand a reality, companies should consider thinking through the following phases of a holistic brand protection strategy:

A key to performing the assessment is to have a framework.

Key to performing the assessment is to have a framework that helps define all the aspects that are necessary for an effective Brand Protection Program. The Brand Protection program model shown at right is one such framework. Teams should assess where there are relative to leading practices and explicitly decide what level of effort or investment is warranted given the size and nature of their specific business problems.

Design: Once the assessment is complete, design requires creating a vision for a more secure future. This step includes comparing the current in-house technology with alternatives in the market place. Often times, there is no single solution for one company that can simply be applied to another company. For example, varied organizational capabilities, unique consumer needs, differences in supply chain constraints, and diverse corporate goals all require a customized solution set.

During this stage, it is critical that the strategic partner be "technology agnostic." There are almost as many technological solutions as counterfeiters. Sometimes as a result of lack of information, solution providers position their technologies as the "right solution" without truly understanding how the proposed solution suits the bigger brand protection strategy.

As an example, a sophisticated "track & trace" system may be of little use for a retailer that has a shrinkage problem.

In such an instance, the organization might be better-off protecting its merchandise with a combination of anti-theft and authentication technologies. To summarize, the design stage needs to consider the entire life cycle of the brand protection solution, including plans for implementation, monitoring and enforcement and total cost of ownership.

Protect: Once the planning and designing have been completed and the technology and/or process improvements have been agreed upon, the recommended solution is rolled-out. Depending on the sophistication of the system, the organization may start with a pilot rather than a full blown implementation. Moreover, it is important to also create contingency plans, internal security checklists, enforcement procedures and comprehensive roles and responsibility models as part of the entire execution.

Monitor: Unfortunately, this phase tends to get the least attention. Companies often come to the conclusion that by installing brand protection technologies, they become safe and impregnable. While this perception may be true initially, persistent counterfeiters can secretly infest the brand by finding back doors and weak links over time. Thus, monitoring is one of the most critical components of an effective brand protection strategy and is the step which maximizes the value of brand protection investment. The biggest threat to an effective brand strategy is not what can be seen, but rather what cannot be seen. Monitoring involves continuous testing and evaluating of the entire product lineup, particularly those products where security solutions have been implemented. This constant check helps brands understand which fences the counterfeiters have breached and which ones are (still) secure.

Monitoring is one of the most critical components of a brand protection strategy.

There are a few reasons why monitoring is overlooked. First, there is often a perception within many organizations that brand protection is insurance. Companies believe that they can avoid expensive liabilities by illustrating that they have "checked the box." An additional contributing factor is that ongoing monitoring tends to be the most difficult part of brand protection. This is primarily because it involves multiple entities outside the company's line of control with many companies viewing it strictly as a line-item expense that can be eliminated during the next round of cost-cutting. To make things even more complicated, many brand protection solution providers consider their responsibility to end after they have sold their technologies to organizations, leaving companies without the guidance, tools or plans to prepare for the inevitable day when that particular technology fence is crossed. Very often, vendors feel that their technologies are simply enablers; how an organization chooses to use the technology is "out of scope." Whatever the obstacles, an effective monitoring plan should be considered an integral part of a complete brand protection strategy.

Brand Protection Program Model					
Categories	Subcategories	Stage			
		0	1	2	3
Authentication and Traceability	1. Authentication Technologies				
	2. Serialization				
	3. Track and Trace				
	4. Tamper Resistance				
Incident Detection	1. Incident Monitoring				
	2. Product Sampling				
	3. Sales and Returns Data Monitoring				
	4. Import/Export Monitoring				
	5. Distribution/Warehouse Audits				
Incident Analysis and Investigation	1. Investigative Staff Roles				
	2. Incident Selection (for investig.)				
	3. Case Management				
	4. Case Analysis				
Agreements and Enforcement	1. Distributor Agreements				
	2. Employee Agreements				
	3. Distributor Contract Enforcement				
	4. Civil Actions				
	5. Criminal Prosecutions				
Business and Metrics	1. Incident Metrics				
	2. Case Enforcement Metrics				
	3. Financial Metrics				

Enforce: As part of the monitoring plan, the brand owners will have collected data about incidents and they need to track these incidents. They need a system to decide what incidents, or collection of incidents, are the most serious and warrant further pursuit. They need to develop and implement an investigative plan. They need to find ways to stop the undesired activity which may take the form of repairing sales channel vulnerabilities, working with customs officials, taking civil actions, or taking legal criminal actions. The elements of the brand protection solution need to provide clear facts and statistics that can support the enforcement process.

Summary: While the phases listed here constitute a blueprint for designing the system, let us now review the different tools that can be used to make this vision a reality. There are five building blocks namely — governance and policies, process, technology, infrastructure, and people. Policies help determine constraints and rules for the future state solution. Process flows help create roadmaps of proposed system functionality, while ensuring efficiency, performance, and effectiveness. Technology is the core enabler of the brand protection solution but must be evaluated using the previously defined policy and process controls. Infrastructure provides the nuts and bolts to hold the system together. Lastly, people drive solution adoption and acceptance, therefore must be considered for any implementation to be truly successful.

Achieving the Vision

While brand owners can certainly envision their needs and desires to drive the thought process, there are many different approaches and solutions for the same problem. For instance, below are a few different methodologies to initiate a brand security solution:

- Conducting a current environment risk assessment thereby refining the existing preventative or protective solutions in place
- Analyzing a brand portfolio to identify which products have the most loss due to counterfeiting and following up with an approach to stop the bleeding
- Investigating supply chain security by conducting sting operations and plugging the gaps with the appropriate legal or strategic actions
- Designing a comprehensive monitoring and enforcement strategy to mitigate IP infringement, black market counterfeiting, and gray market diversion

Tasks must be organized in increments that the organization can reasonably be expected to absorb.

Each phase and component plays an active role in ensuring that all aspects of a high-performing brand are evaluated and executed appropriately. It is important to avoid falling in the trap of relying too heavily on one phase or one component and completely neglecting others — for example, focusing primarily on protection, or relying too much on policies will result in a less than optimal solution.

The underlying theme in all these approaches is how much value is lost due to counterfeiting at the target organization? In other words, what economic models exist to determine the amount of value preserved/created by adopting anti-counterfeiting capabilities? The underlying goal is to allow the brand owner to better understand the scope and magnitude of the problem. Lately, more and more organizations are trying to fight counterfeits and fraud without accurately being able to determine the true impact to the bottom line. Proactive brand owners start by "quantifying the pain" and accordingly allocating resources. For example, does the brand really need a corporate brand protection attorney and a chemical scientist on a full time basis to limit counterfeits or should they allocate their funds on a brand protection solution? Is taking a more minimal approach a viable option? One cannot realistically answer these questions without truly understanding the financials.

Roadmap to Change

Once brand owners understand the strategic and overarching challenges, the journey to implementing a high performing brand protection solution can begin. A team of experienced business consultants and technicians can help maximize value for the host organization and quickly drive change. In fact, one of the first steps should include developing an approach for managing change and related risks.

We recommend convening an executive steering committee to develop and execute on the project charter. For example, is the ultimate charter to reduce liability, realize financial targets, improve profits or build brand awareness? The committee's guidance and ownership helps ensure that these and other similar issues encountered along the journey are resolved, and that communications flow smoothly to convey project status and re-emphasize the benefits of change.

At Kodak, we utilize a phase-gate approach into roadmaps to mitigate risks. At each phase of plan execution, the project value is validated and the completeness of deliverables is reported to all stakeholders. This helps ensure that before the team makes any investment, all decision makers are made aware of the action's value and risks. This also presents an opportunity for corrective action or redirection before additional assets are expended.

Moreover, we believe that work to be performed between each milestone should not overstretch the capabilities of the organization. Instead, tasks must be organized in increments that the organization can reasonably expect to absorb. The plan should also develop contingencies based on probabilistic outcomes to guard against surprises.

This approach enables the brand protection solution to be implemented in an accelerated yet controlled manner. The organization can identify value, prove the model works and easily scale to end state with minimum disruption to current operations. In addition, early trial successes can be celebrated to help maintain momentum.

Proactive brand owners start by "quantifying the pain."

Lastly, to maximize the probability of success, brand owners may consider collaborating with strong partners. A strong partner will have broad experience in all types of brand protection problems in different market verticals. They will have a thorough understanding of the technology, capabilities and cost of available brand protection solutions, and will be able to evaluate brand protection solutions against best-practices criteria for each solution type. A deep understanding of best-in-class technology solutions is derived from experience in the brand protection marketplace and from hands-on experience with brand protection technology development. A strong partner will understand the ramifications of implementing solutions globally and in different manufacturing environments and be able to design and manage an implementation program with appropriate robustness and quality specifications. Here, expertise can be derived from an in-house, global, manufacturing base. Finally, given that the most precious possession of an organization is in question — its brand — the ideal partner is one with the corporate reputation and global presence to stand behind a brand protection solution.

Conclusion

With criminals introducing new ways of committing fraud and attacking a brand, many corporations respond reactively and with limited success. Factors contributing to failure are problem complexity, unclear ownership and perceived low cost of inaction. Quantification of the benefits of a brand protection strategy can be difficult, technical solutions intricate and organizational insight limited. But having a well designed, multi-staged approach to the problem enables brand owners to overcome these challenges thereby creating a holistic and effective brand protection strategy. An optimal architecture should be built around the key building blocks of policy, process, technology, infrastructure and people. Brand owners can minimize implementation risk and maximize solution viability by leveraging the help of an experienced brand protection partner such as Kodak, to act as an advisor and subject matter expert.

For more information about Kodak's security solutions:
Visit www.kodak.com/go/brandprotection
Or email traceless@kodak.com

Eastman Kodak Company
343 State Street
Rochester, NY 14650 USA

U.USR.168.1014.en.02 (K-168)

Kodak