page 2
Cybersecurity essentials for small to mid-size businesses

page 3
Is a patent enough? How to protect your intellectual property

page 4
Traditional office vs. co-working space: Which is right for your business?

Legal Matters®

Business Law
summer 2017

Know the risks associated with using targeted advertising for your business

Many companies employ third-party advertising services that use online consumer data and automated software to place advertisements on websites, in apps and within user-generated video services.

But this wide-reaching marketing tool comes with the risk that your advertisement and brand could be displayed alongside offensive content. Third-party targeted advertising services, such as AdSense from Google and Bing Advertising from Microsoft, offer the ability to exclude targeted ads from pornographic or gambling sites. But beyond that it is difficult to prevent your ad from appearing on a website that you would prefer not be associated with your business. Many times, when an advertising service identifies a user that matches the intended audience of the advertisement, the user will see the advertisement even on offensive sites.

The rise of fake news sites further complicates matters, as new sites are created every day in an effort to reap advertising revenue. In one recent example of the challenges this presents, Allstate saw one of its ads appear next to an article denying the occurrence of the Sandy Hook school shooting on a fake news site.

A bill recently approved by President Donald Trump rolls back proposed restrictions on Internet service providers, making it easier for them sell customer data, potentially including browsing information.

©Adobe Stock

That will serve to increase the amount of data available for targeted advertisement services.

Despite these issues, there are still options for businesses looking to target consumers who will find their advertisement useful and/or appealing.

If possible, businesses should dedicate resources and establish procedures for monitoring the reach of targeted ads. By proactively reviewing an advertisement's analytics, you can reduce the risk of your ad being placed on offensive sites.

continued on page 3

ALLRED, BACON, HALFHILL & YOUNG, PC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

Cybersecurity essentials for small to mid-size businesses

©Adobe Stock

A strong cybersecurity program is designed to protect the confidentiality, integrity and availability of a business's information systems. These systems can include any computer or networked electronic system used by a business, and certain sensitive business and consumer information.

Programs should be designed to perform three primary functions:

1. Identify and assess threats and risks;
2. Protect information systems and sensitive information from malicious use and unauthorized access; and
3. Detect, respond to and recover from cybersecurity "events" such as breaches.

A business's cybersecurity program should be overseen by a designated responsible individual, such as a chief information security officer. This person is responsible for enforcing the cybersecurity policy. Ideally, he or she will be supported by personnel who oversee the core functions of the program noted above.

Detailed cybersecurity policies should address a wide variety of security concepts, including: data classification; asset inventory and device management; access controls and identity management; business continuity; network and physical security; third-party service provider requirements; and incident response procedures.

Businesses looking to protect their information and systems should consider building the following into a new or existing cybersecurity program:

- Written guidelines related to application security to ensure the use of secure development practices for internally developed applications and to evaluate the security of third-party applications.
- Risk-based policies and controls to monitor user activity and detect unauthorized access to or use of sensitive information. Controls may include multi-factor authentication or risk-based authentication.
- Policies and procedures for the secure disposal of sensitive information, consistent with retention requirements under existing laws and regulations.
- Controls, such as encryption, to protect any sensitive information held or transmitted by the business both in transit over external networks and at rest.
- Limited user access privileges to systems that provide access to sensitive information. The business should then periodically review those access privileges and adjust as necessary.
- Written policies and procedures relating to third-party service providers that address minimum cybersecurity standards and risk assessment.
- A written incident response plan for when cybersecurity events occur. This plan should designate roles, responsibilities, decision-making authority and processes for handling such events.
- A plan for vulnerability assessments that includes monitoring and testing to assess the effectiveness of the program.
- Regular cybersecurity awareness training for all personnel.

Once a program is set, you should then conduct periodic risk assessments that review policies, procedures and practices. These assessments should be governed by a written policy that establishes criteria for evaluating identified cybersecurity risks or threats and assessing the adequacy of existing controls in light of those risks.

We welcome your referrals.

We value all of our clients. While we are a busy firm, we welcome your referrals. We promise to provide first-class service to anyone that you refer to our firm. If you have already referred clients to our firm, thank you!

Know the risks associated with using targeted advertising

continued from page 1

Businesses should also establish procedures for quickly removing ads and responding to public criticism if an ad does appear alongside offensive content.

To be proactive, businesses should consider establishing a blacklist and/or a whitelist. A blacklist notes where your advertisement cannot appear. A whitelist is a list of approved sites where your advertisement may appear.

Although the use of a whitelist reduces the reach of an advertisement, analytics can be used to help create a powerful list that still reaches a wide audience while limiting your brand's exposure to and association with offensive content.

Consider other measures of quality beyond just impressions, such as view-through, click-through and abandonment rates. By placing less importance on the raw number of impressions and focusing on increasing the quality and effectiveness of targeted advertisements, you can create more effective ads while offsetting the risk that your advertisement appears alongside offensive content.

Is a patent enough? How to protect your intellectual property

You had a great idea and you started a business around it. Now, you need to protect that intellectual property.

First, check to be sure that your idea is original. Conduct patent and trademark searches early in the development of new products and processes to make sure there isn't anyone else already protecting the same ideas or concepts.

If you do have an original, patentable idea, go ahead and file a patent application. Filing an initial patent application gives you time to develop or sell your idea, complete market research and/or raise money.

Don't hesitate to reach out to a lawyer right away, starting with these first steps. To ensure that any trademark you develop is properly protected, contact a trademark agent for advice about searches and registration.

A lawyer can also give you advice on whether you need to protect your intellectual property in overseas markets. Intellectual property rights, which include country-specific U.R.L.'s, need to be obtained country by country, and not all countries provide the same level of protection.

Cost can vary significantly. For those looking to sell or manufacture in countries beyond the U.S., consider developing a strategy to go after IP protection in a limited number of countries that are most likely to be of use.

Consult a lawyer to decide what your international IP strategy should be and conduct a cost-benefit analysis to see if expanding your IP rights makes sense.

Throughout the process, be sure to keep a log of evidence that records the development of intellectual property, such as dated and signed copies of drawings, drafts or presentations.

While you're working to obtain trademarks and patents, don't forget about related items, such as a company website U.R.L. Unlike a patent, which can cost up to $25,000 to secure, trademarks and web addresses can be obtained relatively cheaply, without assistance. So it's best to secure the U.R.L. you need early on in the process, before someone else does.

Working toward a patent is great, but make sure you understand what rights it will give you. A patent does not give you the right to produce something, but rather the right to prevent someone else from producing what your patent covers.

And even if you have a patent, there's no guarantee someone won't try to get around it. Patent trolls, or people who collect patents but don't make anything and instead make money filing lawsuits against real businesses, are on the rise. The term was coined as a result of a lawsuit between NTP, a small holding company, and Research in Motion, which makes BlackBerrys. The dispute centered around NTP's patent for wireless email delivery, something Research in Motion eventually would pay millions of dollars to license.

Even though there's no guarantee that you will win if you engage in a legal battle, it's often worth prosecuting to protect what's yours. The more evidence and documentation you've collected along the way, the better. Consult your lawyer to help identify IP breaches and decide when it's worth going after offenders.

To stay on top of all potential issues, it's worth creating a policy for all of your intellectual property, including all patents, designs, trademarks, copyrights and domain names. Then, use contracts to help prevent theft. Ensure all your employment and consultancy contracts clearly state your ownership of any intellectual property developed for you.

If you hold copyrights for certain materials, make sure you add the copyright symbol, your name and the creation date to emphasize they are protected.

As your intellectual property grows and expands, make sure to keep assessing things at every stage of development. For physical products, it may be worth protecting new designs for the appearance of all or part of the product with stronger design registration.

Working toward a patent is great, but make sure you understand what rights it will give you. A patent does not give you the right to produce something, but rather the right to prevent someone else from producing what your patent covers.

ALLRED, BACON,
HALFHILL & YOUNG, PC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

Traditional office vs. co-working space: Which is right for your business?

Collaborative work environments with shared spaces are an increasingly popular take on traditional office space, but can come with less than ideal leasing terms.

©Adobe Stock

Most co-working spaces operate using an occupation license agreement that allows members to use the space for a particular purpose or set of purposes. But it is much easier for a landlord to revoke a licensee's right of access to than it is to evict a tenant.

A commercial leasing agreement for traditional office space provides tenants more rights and a greater level of security. Such leases can be overly restrictive for startup operations planning to grow quickly, however. Those with smaller teams and budgetary constraints may benefit from the collaborative environment and reduced costs a shared space can provide.

If you're considering a license agreement for shared space, consider the following:

- Is there an indemnity clause in the event of theft or lost property, or will you need your own insurance to cover these items?
- Are there restrictions on web usage, printing facilities, use of common areas and hours of access?
- What are the membership fees and what amenities do they provide access to?

For those considering a more traditional space and subsequent commercial lease agreement, consider the following:

- Are you allowed to sublet or license the premises to capitalize on the space if desired?
- Does rent include any other utilities or services?
- Will the lease term match the business needs?
- What are the permitted uses and are there any relevant zoning laws worth noting?
- Does the lease contain an option to renew? An option to renew is a clause in a lease agreement that gives tenants the option to extend their tenancy for an additional term. Typically, a tenant looking to exercise an option to renew should provide the landlord written notice 3-6 months before the lease expires.