INTELLECTUAL PROPERTY (IP): SAFEGUARDING CORPORATE ASSETS IN THE DIGITAL AGE

INTRODUCTION

Intellectual property is a broad categorical description for the set of intangible assets owned and legally protected by a company or individual from outside use or implementation without consent. An intangible asset is a non-physical asset that a company or person owns. It is usually also referred to as creations of the mind, such as; inventions, literary and artistic works, designs, symbols, names and images used in commerce.

The concept of intellectual property relates to the fact that certain products of human intellect should be afforded the same protective rights that apply to physical property, which are called tangible assets. Most developed economies have legal measures in place to protect both forms of property. Intellectual property can take many forms, and each form is protected differently. The different forms of intellectual property are; copyrights, trademarks, patents and trade secrets.

The safeguarding of Intellectual Property therefore, is of growing importance in many countries of the world due to its significance in the social and economic life of any nation. In most developed nations of the world, intellectual property rights of creators and inventors are duly protected by law. Such adequate protection of intellectual property assists the government in curtailing the activities of violators, counterfeiters, and imitators of intellectual works. By this measure, protection of intellectual property rights (IPR) will foster economic growth for the nation and value creation for intellectual works.

THE LEGAL FRAMEWORK FOR IP IN NIGERIA

There are several laws regulating the different types of Intellectual Property in Nigeria. However, there are three (3) major laws relating to Intellectual Property presently in Nigeria, they are **The Copyright Act**, (Chapter C28 Laws of the Federation of Nigeria 2004), **The Trademarks Act**, (Chapter T13 Laws of the Federation of Nigeria 2004), **The Patents and Designs Act**, (Chapter P2 Laws of the Federation of Nigeria 2004).

There are four (4) categories of IP protection in Nigeria today which are; copyright, trademark, patent and industrial design. Although not governed by any statutes, another Intellectual Property recognized in Nigeria is Trade Secrets.

UNDERSTANDING CORPORATE ASSETS AND THEIR SIGNIFICANCE

Corporate assets in the digital age refer to intangible assets that hold value and can be protected through intellectual property rights. These include:

1. Software codes, algorithms, and other digital innovations that can be protected as trade secrets or patents.
2. Digital media such as images, videos, and audio recordings that can be protected by copyright.
3. Literary and artistic works in digital form, including website content, that can be copyrighted.
4. Digital brand assets like logos, domain names, and online presence that can be trademarked.
5. Other unique digital content or data that provides competitive advantage and value to the business.

These corporate assets represent intangible intellectual property that holds significant value for companies. Protecting this digital IP is crucial to safeguarding a company's competitive edge and brand reputation.

In today's fast-paced, digital-centric world, safeguarding your business has transcended the mere physical locks and alarm systems. The digital age brings with it a plethora of opportunities as well as challenges. Protecting your company's digital assets, ensuring data privacy, and staying ahead of cyber threats have become indispensable parts of running a successful business.

HOW TO SAFEGUARD CORPORATE ASSETS

Below are some strategies that can be used to effectively protect and preserve corporate assets in this digital age:

1. **Backup and Recovery Strategies**

As the internet becomes increasingly integral to operations, businesses face a heightened risk of cyber-attacks. From sophisticated phishing schemes to ransom ware attacks, the arsenal employed by cybercriminals is both vast and evolving. Understanding these risks is the first step toward protection.

In the unfortunate event of a data breach or loss, having a robust backup and recovery strategy is essential. Regularly backing up data ensures that your business can quickly recover without significant downtime, keeping your operations running smoothly and mitigating potential losses.

2. **Data Privacy Laws and Regulations**

In addition to implementing protective measures, it's crucial to stay informed about data privacy laws and regulations, which vary significantly across different jurisdictions. This

knowledge not only helps in compliance but also in assuring your customers that their personal information is protected, thereby building trust. For example, the United States (US) has some asset protection laws in place, such as, Securities Act of 1933 and Securities Exchange Act of 1934. Its legal system and the risk of lawsuits pose challenges for breaches, especially for residents within the country.

3. **Creating a Response Plan for Cyber Incidents**

While prevention is preferable, being prepared for a cyber-incident is equally important. Having a detailed response plan in place ensures that your team knows exactly what to do in the event of a breach, minimizing panic and confusion. This plan should include steps for securing any breaches, assessing the scope of the damage, communicating with stakeholders, and reporting the incident as required by law.

As cybersecurity threats continue to evolve, so must your approach to employee education. Beyond baseline training, continuous awareness programs can keep cybersecurity at the forefront of your employees' minds. Engaging training materials, simulations of phishing attacks, and updates about the latest cyber threats can empower your staff to be the first line of defense against hackers.

4. **Advancements in Cybersecurity Technologies**

Keeping abreast of advancements in cybersecurity technologies, without references to specific products, involves understanding new methods of protection. This could include encryption technologies, block chain for secure transactions, and artificial intelligence in detecting potential threats. The goal is to ensure businesses adopt a proactive rather than reactive approach to cybersecurity.

One simple yet effective way to enhance cybersecurity along these lines is by utilizing Multi-Factor Authentication (MFA). MFA requires users to provide two or more verification factors to gain access to a digital resource, making it harder for attackers to breach your systems. This added layer of security can protect against various forms of cyber-attacks, including those that exploit weak or stolen passwords.

Regular security audits are also vital in identifying vulnerabilities within a business's digital infrastructure. By systematically examining its IT environment, it can uncover potential weaknesses and address them before they can be exploited by hackers. These audits can include penetration testing, security control assessments, and an evaluation of the organization's compliance with relevant cybersecurity standards.

CONCLUSION

Securing a business in the digital age is a multifaceted challenge that requires a comprehensive approach. By understanding the risks, fostering a culture of cybersecurity, staying informed on laws and advancements, preparing for the worst with backup and recovery strategies, and having a clear response plan, one can significantly mitigate these risks. The digital age is here to stay, and by taking these steps, businesses will not only survive but thrive.