5 Ways Outsourcing App Development Security Will Help You Cut Costs

nimble.com/blog/5-ways-outsourcing-app-development-security-will-help-you-cut-costs/

IT managers today are faced with many tasks and not enough time to complete them all. While these individuals are primarily tasked with ensuring that their top developers efficiently write code lines, they are also often regarded as the responsible parent in charge of maintaining application security. Given that web applications often entail the transfer of secure information, regulatory requirements are generally the norm. As such, identifying vulnerabilities and company weak spots shouldn't and can't be overlooked.

Knowing this, should code security protocols fall under the job description of your headphones-friendly web developer?

Below are 5 ways outsourcing app development security will help you cut costs both now and in the future:

1. Better use of time. With the need for developers to consistently keep up with coding, outsourcing security will leave them with the ability to focus on what they do best. Plus, this should leave your company employees with more time to improve existing projects, work on customer retention, and take on additional clients.

2. Targeted technology. Trusted IT companies have produced technologies specifically catered to providing advanced security analysis and scanning uncompiled code. Some, including CyActive, offer technologies that attempt to predict and prevent potential threats ahead of time. Managers today are concentrating their efforts on locating precise technologies that can better serve their company's overall performance.

3. Trusting professionals. There are companies whose specific mission is to ensure that web applications are secure and reliable. Checkmarx for instance, is a premier and rapidly growing example of this type of service provider. Their software helps identify source code security vulnerabilities impacting leading companies such as Deutsche Telekom and LivePerson.

4. Potential cost of 'business-as-usual'. If you choose to run your app security operations according to a daily routine, you may find yourself later addressing mishaps and security failures. This may prove costly in terms of time lost, client distress, and potentially even more critical security implications. Furthermore, this may also be

detrimental to your company’s image in the eyes of investors and customers alike.

5. Reputation building. By partnering up with an external security provider, especially one well received by experts in the industry, your company or product will be synonymous with security and reliability. This positive PR may lead to new clients and a general increase in brand awareness and market presence. As such, adopting these technologies has both security and market value for your business.