

Information Security – Growing Problem Not Only for Hospitality Industry

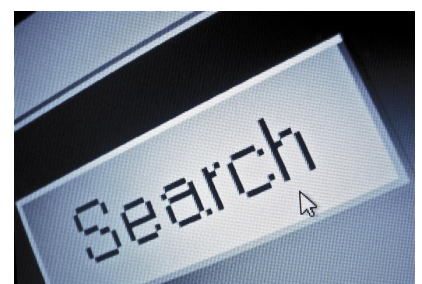
As security programs have advanced, very few organizations are truly ready for tomorrow. New and evolving models of information security are really required to keep up with the problems that you will face today. These updates make sure that our evolving information security models keep up with today's challenges.



Many hotel executives are beginning to increase security spending and safeguards, processes, and strategies. However, modern day foes continue to outrace the upgrades, according to the Global State of Information Security Survey 2014, as released by PWC US in conjunction with CIO and CSO magazines.

Their survey revealed that, though there are many positive security improvements for today's companies, they are still lagging behind security opponents. Per Mark Lobel, a PWC Advisory Cybersecurity principal, this poses significant problems for future security. According to Lobel, it is of the utmost importance that we constantly and actively evaluate and update security plans, strategies, and practices to keep up with threats today. Without this flexible approach, companies will be ill prepared for a security attack or threat. These attacks are becoming increasingly more effective, complicated, and damaging for companies.

According to the global survey, which reached over 9,600 executives, security incidents that were detected in the past year have drastically increased. At last check, the estimated percentage was 25 percent. On that note, it was seen that those who were unaware of the volume of security incidents doubled.

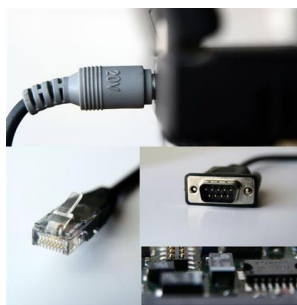


Bob Bragdon, publisher of CSO, noted that with today's increasing threats, all organizations including the

hospitality industry must be ready with new technologies and plans that will keep an eye on their network. They must watch all applications and data for odd or anomalous activity that may point toward a security threat.

With smart phones and tablets, it has become common to bring your own device everywhere. However, between these items and the preponderance of Cloud computing, these have elevated security risks. However, efforts to create and implement mobile security programs have lagged well behind the increasing mobile device use. Though 47 percent of respondents regularly use cloud computing and storage, 59 percent of those have said that they are improving security and 18 percent have not included Cloud computing in security provisions. The survey noted that most implemented new security protocols like VPNS or firewalls, they are unlikely to use real-time intelligence tools to monitor risks and in-progress security threats.

It is absolutely essential that companies rethink and renew their security policies. They must be integrated with the needs of the business and made a priority by the company's top executives. Security threats must be taken seriously, through collaboration to improve security and evaluate risks. However, only 50 percent of those interviewed said that they collaborate to work on their security problems.



According to David Burg, PWC's Global and US Advisory Cybersecurity Lead, integrated security should be the cornerstone of a company's overall agenda and culture. They need to build and sustain security awareness, though this will require full support of the top executives. It is impossible without that support.

Per the survey, the top three obstacles blocking improved security were insufficient funding, a lack of future vision for business needs, and a lack of support and leadership from the top executives.

Gary Loveland, another Cybersecurity lead with PWC Advisory, noted that you cannot keep up with today's threats and challenges if you are using yesterday's technology. A new, novel model of information security and technology needs to be developed; one that keeps new threats and knowledge in mind.

Current and former employees are noted as a major security weakness and source of security incidents. Though many believe that nation-states are the cause of most threats, very few respondents recorded them; only 4 percent, compared to 32 percent that complain of hackers as a source of outside security threats.

Date: 2013-09-30

Article link:

<http://www.tourism-review.com/travel-tourism-magazine-information-security-is-a-serious-problem-for-hospitality-and-other-industries-article2201>