

Headline: "Hackers can't be wished away in India now"

Publication: iGovernment

Date: 30th December, 2011



The screenshot shows the iGovernment website interface. At the top left is the logo "iGovernment enabling good governance". A navigation bar contains links for Home, eGov, Technology, Policy, Economy, Education, Health, Infrastructure, Agriculture, and Human Resources. Below the navigation bar, the page is dated "Friday 30 December 2011" and has the tagline "Government 2.0: The Road Ahead". The main content area features the headline "Hackers can't be wished away in India now" in red, followed by a sub-headline: "Government and private concerns in the country need to fortify their information security systems to check cyber intruders, says AGC Networks VP". The article is dated "Submitted on 12/30/2011 - 08:14:25 AM" and written by "Prithwi Raj Sinha". A portrait of Atul Khataavkar is shown next to the text. The text states: "New Delhi: The information security scenario in both government and private sectors is far from encouraging because of lack of awareness and understanding of data security, AGC Networks Vice-President (IT Governance, Risk and Compliance), Atul Khataavkar says. Khataavkar, in an interview with iGovernment, said that the year 2011 has been the year of hackers, with major companies such as Sony being attacked in the first six months and Stuxnets entering into Iran to affect its nuclear facilities. According to Khataavkar, over 6,000 websites ending with .gov.in and co.in URLs and around 4,000 .com sites were hacked in 2011. This clearly shows the level of information security systems that India has in place. AGC recommends that significant changes are required at the top level of an organization - from CEOs to CFOs - who actually sanction the budget."

"Hackers can't be wished away in India now"

Government and private concerns in the country need to fortify their information security systems to check cyber intruders, says AGC Networks VP



New Delhi: The information security scenario in both government and private sectors is far from encouraging because of lack of awareness and understanding of data security, AGC Networks Vice-President (IT Governance, Risk and Compliance), Atul Khatavkar says.

Khatavkar, in an interview with **iGovernment**, said that the year 2011 has been the year of hackers, with major companies such as Sony being attacked in the first six months and Stuxnets entering into Iran to affect its nuclear facilities.

According to Khatavkar, over 6,000 websites ending with .gov.in and co.in URLs and around 4,000 .com sites were hacked in 2011. This clearly shows the level of information security systems that India has in place.

AGC recommends that significant changes are required at the top level of an organization - from CEOs to CFOs - who actually sanction the budget.

Khatavkar said the common perception of the Indian top-level management is that this phenomenon of hacking and information security is limited to the US and they would not get affected at all. Lack of pro-active decisions due to low-level of commitment among the top management is another hindrance in the acceptance of information security solutions, he added.

Giving the example of RBI which gave certain mandates for information security in banks, the AGC Networks' VP recommended that similar kinds of regulations and compliances should be created by the government for enterprises or organisations for information security in their information infrastructure.

Earlier, the information security phenomenon was restricted to private enterprises, but it has now moved to government sector with governments taking many initiatives such as technology implementation in their infrastructure or e-Governance, according to Khatavkar.

Moreover, the advent of high-end mobiles devices, such as smartphones and tablets, has further pushed this phenomenon to individuals.

In terms of unified communication, the biggest challenge is that people or organizations are not aware of the threats and risks that it poses to them, though they have UC infrastructure in place. Earlier it was analogue but today it is IP based; IP based phone can be monitored from anywhere in the world, Khatavkar said.

Though government department or enterprises have migrated or planning to migrate to IP based communication system, they are not aware of where they are getting into and what kind of preparedness they have in place, he added.

"We have developed a separate auditing practice for auditing unified communication. The only way to improve information security is to regularly monitoring and auditing," he adds.

Government is not focusing on UC heavily, but at the same time biggest risks are coming from social media, according to Khatavkar.

The government or organizations are not really well equipped to tackle threats from social media, but an attacker is quite capable to attack as it is more aware of the system. The flourishing of social media websites is calling for more awareness on information security, the AGC Networks VP reiterated.

Though there are many high-end technologies available today, an attacker doesn't need to use these high-end technologies to hack information from social media, as about 92% of these threats are with the soft targets, he said.

According to Khatavkar, humans are considered as the weakest links in the system, and training, awareness creation, building processes, and ISO27001 help governments to standardized processes across organizations.

Also, AGC implements many technologies, such as two-factor authentication, encryption, and VPN to mitigate information security risks.

Indicating that there are many challenges in video conferencing, the AGC Networks VP said firstly many people are still not comfortable with the whole concept of UC, and secondly, bandwidth is also an issue for its acceptance.

Compared to other countries like the US, the comfort level to use VC in India is less or at the nascent stage.

According to Khatavkar, AGC is integrating and hiring more practices, including security business and delivery of security – IT security, IT governance, and compliance, for the past one year. The company will touch \$500m in revenues this year.

The company majorly focuses on the government sector, and has a separate team to talk to the government to help them start information security processes within their set up, Khatavkar said.

“From security perspective, we have already worked with very sensitive organizations, including Indian Navy, Nuclear Power Corporation, and provided them with advanced, sophisticated, and customised information security solutions,” he added.

“We are also into consulting and help government customers to decide on the relevant solution that will fit their structure as well as the bill. They include technology infrastructure and people involvement as well.”

The company also helps the government in framing policies and strategies, and training people to drive info security within the organization, while ultimately helping them to achieve ISO 27001.

Link: <http://www.igovernment.in:81/site/%E2%80%9Chackers-can%E2%80%99t-be-wished-away-india-now%E2%80%9D>