Computer Society of India™ Since 1965

NASHIK CHAPTER: KNOWLEDGE SHARING SERIES: ARTICLE 665: 11 SEPTEMBER 2023

Getting in the right mindset for security transformations

Marcus Law

Getting in the right mindset for security transformations

Taking a new approach to security can help avoid resistance and even resentment from cybersecurity teams, according to DevSecOps expert Larry Maccherone

Staffing issues in the cybersecurity workforce are well known. (ISC)2 research estimates the size of the global cybersecurity workforce at 4.7 million people, but warns the industry faces a worldwide gap of 3.4 million cybersecurity workers.

And with reports suggesting that organisations are being too slow to patch security concerns, implementing DevSecOps can be a solution to organisations looking to tackle security issues.

As Deloitte explains, DevSecOps fundamentally transforms cyber and risk management. Short for development, security, and operations, DevSecOps automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.

“The purpose and intent of DevSecOps is to build on the mindset that everyone is responsible for security with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required,” describes Shannon Lietz, co-author of the “DevSecOps Manifesto.”

As Larry Maccherone, DevSecOps Transformation Architect at Contrast Security told Tech LIVE Virtual in June, taking a fundamentally different approach that creates a good sense of trust between security and development groups can actually move the needle in reducing cybersecurity risk.
“In the world of application security today, we tend to beat people up with it. We tend to not actually trust them and help them become worthy of that trust, especially the security group in relation to the development group.”

Organisations need to move away from a gatekeeping approach to security

When scaling DevSecOps transformation in the enterprise, Maccherone argues that organisations need to move away from a gatekeeping, confrontational approach to application security. The first challenge in pulling this off is to get the mindset right.
“Today in some security teams, there is this approach of the ‘beatings will continue until morale improves’,” Maccherone says
As a result, this process can build up significant resistance and even resentment among development teams.
“Basically they're trying to find problems in somebody else's work,” Maccherone says. “This doesn't scale with the accelerating pace of development. So that's a common problem with this gatekeeping policing auditing approach to application security.
“That's one problem that almost everyone recognises. But I actually think there's some more harmful attributes to this approach, that they're actually more significant.
“And it’s the fact that this approach just can't keep up. It's soul-crushing work and it's time consuming. When I started at Comcast, there were roughly the equivalent of 40 full time people essentially doing this cajoling, gatekeeping work all day long.
“The problem is that there's a high turnover rate in the first 90 days that people come into a job that has this because it's very, very difficult and it's not a lot of fun. And the worst part about it is that the people that stay past those 90 days are the ones that maybe enjoy calling someone's baby ugly all day long.
“That does not lead to a good, healthy group that has to interact with developers all the time. It's confrontational and enforcing policy is confrontational. And that's also not fun and doesn't feel good to everyone.”
This, Maccherone explains, can result in less effective operations.
“At best, you often get a checkbox-like response. What's the minimum I can do to get you to go away? And that usually means it's not very effective. They're not sensitive to the context that they're running in. They're not adapted to modern approaches to development. If you only enforce the ones that are appropriate, then that seems arbitrary. And the developers start to think, if they don't have to do some of these policies, why should they have to do any of the others?
“But if you tried to enforce all of it, it would be too much information. It's depressing, as a solution, and it doesn't work.”
As a result, organisations can take a new approach, enabling true DevSecOps.
“DevSecOps is about empowering engineering teams and collaborating with engineering teams,” Maccherone explains. “But that isn't enough. It's not even enabling them because you can lead a horse to water. That's the enabling part. But you can't make them drink.
“I don't want them to be made to drink. I want them to be able to lead themselves to water and drink. Empowering is the right word here to take ownership of the security of their products. You can't have DevSecOps without DevOps.”

Implementing a culture of DevSecOps

This, Maccherone explains, involves implementing a culture of flow feedback, of experimentation and of learning. Better collaboration between development, security, and operations teams improves an organisation’s response to incidents and problems when they occur.

“This is the real definition of DevOps and it and if you aren't actually buying into these concepts, you're not really doing DevOps in my mind.”
Ultimately, this process aims to continue to provide value, delivering security at speed,” Maccherone concludes. “We can never forget that roadmaps have to have to be maintained, they have to be met and we have to keep delivering software. We can't stop the presses too, to do some security.
“We have to hopefully accelerate security in the long run,” he adds. “I don't like to talk about policies, I prefer to talk about practices because the policy is something somebody says you must do.
“Practice is what you actually do. And so I want people to adopt practices. I want development teams to adopt practices, to identify a list of practices that you want to encourage, and ultimately empower engineering teams to adopt."

Video of The Week

Explore some related information to above article at following link.

https://www.youtube.com/watch?v=zOMFXoKH5uU

https://www.youtube.com/watch?v=jsxiII2p4Hw

https://www.youtube.com/watch?v=vWN0_40LU2c

https://www.youtube.com/watch?v=mmvvMtMqcqI

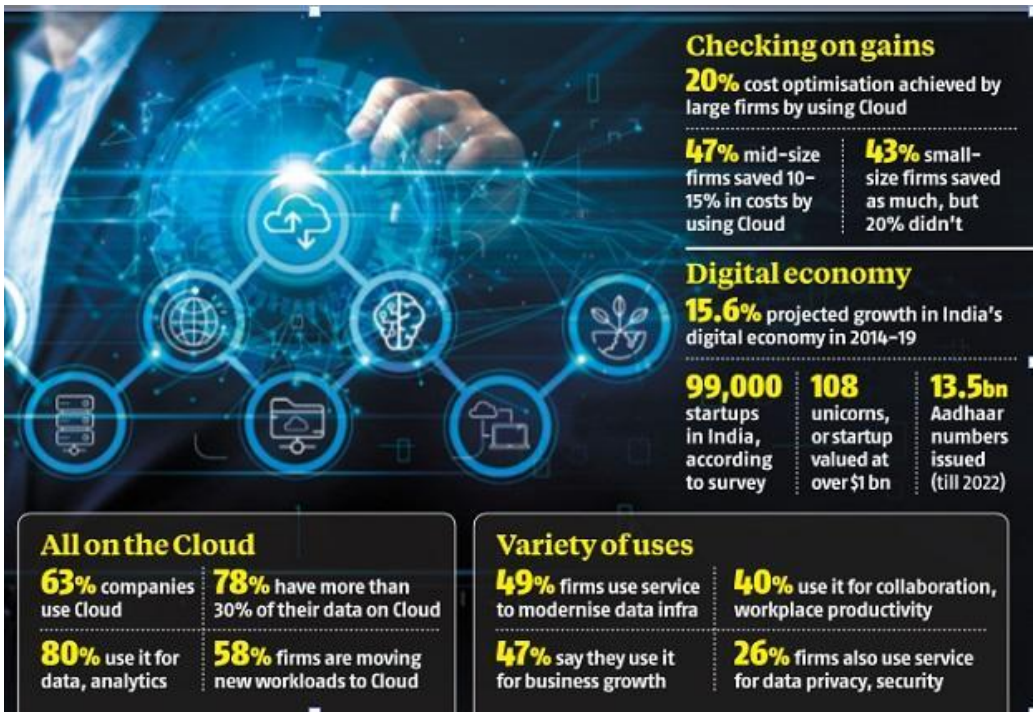
https://www.youtube.com/watch?v=66tbFv3R1xA

News of The Week

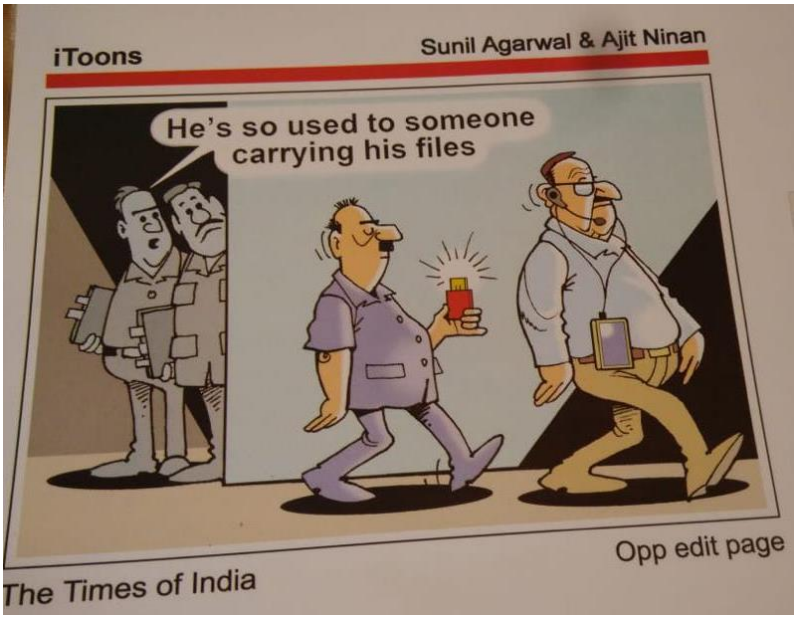
Nearly 63% firms use cloud services for monetizing data and insights

20% cost optimisation achieved by large firms by using Cloud

Indian companies are scaling up their investment in cloud computing, the on-demand delivery of information technology (IT) resources over the internet, as they seek to improve revenue and services. As many as 63 per cent companies use cloud services for monetising data and insights, according to a report by EY, the international consultancy, and business chamber Ficci. The report surveyed 700 firms in more than 20 sectors in seven Indian cities.



E Toon



MR AJIT NINAN DIED IN LAST WEEK.

Feedback/Contribution of articles is appreciated at: nasikcsi@gmail.com

To know more about forthcoming programs and events, please do visit chapter website