BEING RESILIENT

SECURITY IN THE ERA OF REMOTE WORKING

Infosys®

Navigate your next

BEING RESILIENT. THAT'S LIVE ENTERPRISE.

Security in the Era of Remote Working

In an effort to decode the ‘New Normal,’ Infosys recently conducted a successful webinar discussing ‘Security in the Era of Remote Working.’ The webinar brought together 250+ industry leaders from across the globe apprising them on the security challenges that come with remote working and how CISOs need to be ready with remedial measures to address them.

Speakers

Mohit Joshi
President, Infosys Ltd.

Vishal Salvi
CISO & Cybersecurity
Unit Head, Infosys Ltd.

Dr. Martijn Dekker
CISO, ABN AMRO Bank

Audience demography

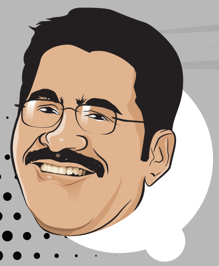
250
Decision makers

400+
Audience

The Context – Remote Working and its Challenges

Our lives have changed dramatically in the past six weeks as we moved to working from home. As a CEO of a client organization mentioned that historically they've had 20,000 people working in 30 offices globally and suddenly they moved to having 20,000 people working in 20,000 different offices.

Looking at what was happening in China and Iran, we started to plan in advance for an eventual lockdown situation which was massive because at Infosys we have 240,000 employees. We started hyperscaling our backbone infrastructure to enable remote working and saw a 4.5x and 10x increase in our concurrency and bandwidth respectively.



Measures of the lockdown in most countries around the globe were aimed at ensuring safety and business continuity.

Learning and Responding Swiftly

There are two broad areas of concern, the first being working from non-approved devices. This includes untested remote access infrastructure which does not meet normal company standards. There's also the need to modernize legacy systems to make them secure and accessible remotely.

The other more important issue is the behavioral factor. A lot of the security loopholes from the past are due to poor computer security practices.

While the world was grappling with the pandemic, the threat actors were clearly not. They were looking at this as an opportunity to exploit the fragility of this massive transition that the whole world was going through. We saw a significant jump in spams, malicious URLs, ransomware attacks, and phishing sites.

Jan to Mar 2020 cyber threat trends

907k	total COVID-19 spam messages
48k	hits on malicious URLs
522k	active phishing sites as of Mar 20
220%	increase in spam from Feb to Mar 20
260%	increase in malicious URLs from Feb to Mar 20
148%	increase in ransomware attacks
350%	increase in phishing sites from Jan to Mar 20

At ABN AMRO, we quickly installed a daily crisis team to ensure effective decision-making as we began to make an increased number of risk decisions. Data confidentiality and integrity were important but availability was most critical. As the threat landscape changed, many vulnerabilities changed and we had situations where people were working from homes using very weak technologies accessing the corporate network via public networks. This is the situation that many companies quickly moved into.

Shift in Priorities

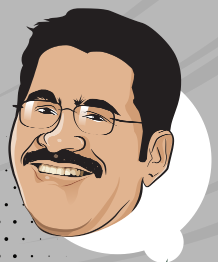
Initially, the main focus was on human safety and mobilization of resources. Now this is moving to security and productivity. It also raises the need for stringent security considerations. For a lot of our clients in the healthcare and banking space, for instance, this was the first time that people were moving to a work from home environment and there was a degree of urgency around it. But now the focus is on ensuring that there is a high degree of security built into the entire remote working model.

Traditionally the FS sector has been extremely sensitive towards allowing a camera phone into the offshore development centers and rightly so because there are liabilities and regulations involved with it. Now with remote working, we need to recalibrate and look at compensatory controls so that work is not affected. In manufacturing, there are advanced persistent threats, not necessarily related to disruption but around discovering who is installing malware and infiltrating data. This is something every industry will calibrate based on the risk profile but a bare minimum is required for everyone.

I think CISOs should now be focusing on the slower processes like how to patch or harden new endpoints. What's your strategy to push patches over public networks? You may not notice these immediately but you will have to start strategizing around them. Figure out what threats can migrate with your supply chain to your company as everyone is now managing a new perimeter and how to sustain this model of working because we're going to be in this for a while. So after you are done transitioning, address these slower processes.

Balancing Security and Productivity

Not many employees are used to the remote working model so it is important that we don’t just address the technical security implications but also the related human issues such as how they perceive and respond to risks. For the first time you have had organizations setting up virtual contact centers and processing centers so you have a lot of operations staff working from home. They are used to a lot of on-site supervisory help but many of them are not familiar with the technology and the collaboration tool. This is a significant issue.



You need to have a balance of security. If the laptop is hardened to the point that it does not allow you to do your normal work, it's of no use. So you need to ensure effective and transparent security while being aware of the requirements of seamless access enabling efficient communication, collaboration, and interaction. I think that balance is very important.

Best practices

- ☑ Hyperscale user concurrency and bandwidth
- ☑ Amplify helpdesk capabilities with intelligent self-service
- ☑ Implement transparent security controls so that user experience is not impacted
- ☑ Prevent bad security behavior/decisions

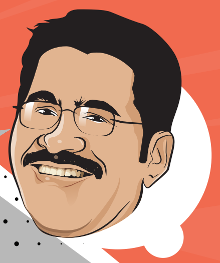
A lot of processes needed immediate attention to ensure seamless remote working. Most of us would have been doing things like scaling of the VPN capacity or providing MFA tokens to all employees and possibly to suppliers. Then there was the logistical problem of getting them to the employees which required extension of many parameter controls.

You have to quickly recalibrate your defenses. While people are working from home in different environments, it's important to educate them on secure remote working and the use of new tools. So raising this awareness is critical.

Workplace of the Future

I think the long-term consequences of how we work as people, how we work in teams, in constrained environments and how we juggle multiple balls with the family and with persistent threats, will provide ample fodder for research in the coming decade.

Building security as a foundation should be the mantra of the future. Security is a very fundamental enabler for business. So I guess secured by design becomes very important and for that to be a reality, the future of security will be about how nimbly you can adapt and respond to the post COVID-19 scenario.



It's interesting to see what type of people will form a successful team in this new setup. We should at least reassess and reconsider the idea of a successful team and understand the type of people who make up such a team. Does this new setup demand something else? I think that is something we should be looking at because the attackers will also be looking at exploiting this behavior of people in the new working model.

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next