CYBER DEFENSE MAGAZINE

eMAGAZINE

SEPTEMBER 2022

In This Edition

Critically Important Organization?

Federal Progress On Zero Trust: A Report

Information Warfare and What Infosec Needs to Know

…and much more…

MORE INSIDE!

Protecting The Enterprise in The Digital Era

What Organizations Need To Know In The New Workplace

By Anurag Lal, President and CEO, NetSfere

Over the past two years, the entire globe has experienced a takeoff in the digital era - specifically within the enterprise. Naturally, cybersecurity concerns have advanced alongside these developments, and a myriad of issues and concerns, especially regarding data and privacy, continue to rise to the surface. As the workplace becomes increasingly decentralized with remote and hybrid work becoming the norm, cybersecurity must move to the forefront, becoming a top priority for enterprise leaders.

Pre-pandemic security efforts are no longer adequate in maintaining the utmost protection of company information. In order for organizations to fortify the role cybersecurity plays in both their digitization efforts and the overall success of their business, there are crucial elements that must be considered and reflected – and acted – upon.

Employees are your weakest link.

Almost 100% of all data breaches within organizations are a result of human error. With employees no longer under the same roof, IT control becomes increasingly more difficult for enterprises with employees across not only multiple Internet networks, but in many instances, different states. Additionally, with the

growing popularity of BYOD (bring your own device) policies, security levels are more likely than not significantly lower than in a traditional, pre-pandemic office setting as IT cannot fully control personal devices to the same standard. Employees are accessing company emails, websites and other materials on their personal cell phones and laptops that have little to no protection compared to their work devices.

How do we ensure that remote and hybrid employees and their work are protected equally? The answer is simple: education.

It is up to enterprise leaders, IT and human resources departments to continuously supply and deploy educational materials for employees on cybersecurity best practices. Additionally, it is important to note that trends in phishing scams are becoming considerably more sophisticated, appearing more discreet and often targeting new channels, like SMS. It is the employer's responsibility to equip its employees with the knowledge to distinguish such attacks, report them to IT and not interact or engage with them. Companies should also consider a course or class on the matter, repeating it annually and/or with new hires to ensure cyber safety is a priority for each team member.

Implement the necessary tools and systems to protect data at every level.

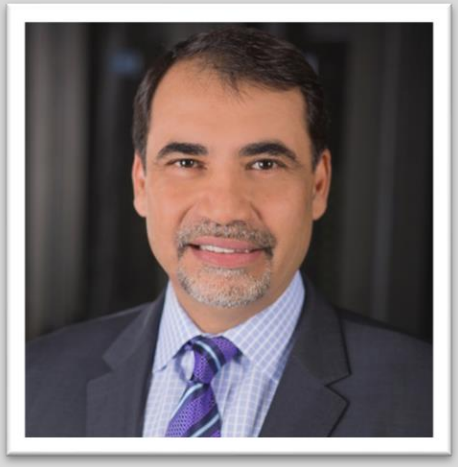
Your employees may have all the tools they need to engage safely at work, but that alone is not enough.

Any platform or channel where sensitive data, information, plans, documents, records and other confidential files are shared must be protected at every entry point. There are many types and tiers of encryption floating around, but end-to-end encryption absolutely is the gold standard. With the message being decrypted only on the device of the sender and recipient, the chance of an attacker accessing information is depleted. This is vital in the remote era when employees are communicating on digital channels like email and instant message, especially when using their personal devices. Industries like healthcare and finance are more susceptible to attack due to highly sensitive and valuable personal information and records as well as outdated and inefficient systems. In light of recent events overseas, these sectors, among many others, should consider deploying fully encrypted, compliant collaboration channels, ensuring that information is being exchanged securely and end-users are protected as well.

It is also worth enterprises considering adopting a zero-trust framework to further limit employee access to company information and decrease the risk of a human error-related breach. This model requires network users to be verified at every entry point and gives them access to only what is required to perform a task or role. With a zero-trust implementation, unverified users are immediately denied entry to the network, providing a sophisticated level of security to the enterprise.

The digital technologies and best practices being implemented by enterprises today are shaping their futures for a safer, more efficient and successful tomorrow. It will pay off in multitudes to take a proactive approach to the protection of your company and teams. Invest in your employees. Safeguard your company data, devices and communication channels. Take no risks.

About the Author



Anurag Lal is the President & CEO of Infinite Convergence Solutions. With more than 25 years of leadership and operating experience in technology, mobile, SaaS, cloud and telecom services, Anurag leads a talented team of innovators who are transforming everyday messaging technology into secure, highly scalable communication platforms that can be leveraged across a variety of markets and segments. Appointed by the Obama administration, Anurag also previously served as a Director of the U.S. National Broadband Task Force (part of the Federal Communications Commission). A frequent contributor on wireless connectivity, broadband and related security issues, Anurag has received various industry accolades, including recognition by the Wireless Broadband Industry Alliance in the U.K. for exceptional individual contributions to the wireless broadband industry. Anurag can be reached on LinkedIn at https://www.linkedin.com/in/anuragl. For more information about NetSfere, please visit https://www.netsfere.com/.