Rajeev Mamidanna,
President, ISODA

Hello Fellow
ISODA Colleagues!

Yet another month has flown past us quickly as we approach the calendar end of the year. There has been a flurry of activities across the country and all the regions have picked up pace. Both in business as well as for the association.

We bring to you again, some very interesting topics under the tech buzz section, where we cover articles written by our own colleagues around preparedness against Ransomware (Mr. Muneer Ahmed) and management of large distribution organization (Mr. Ashok Kumar). On the Regional Meets front, we cover West and South with information from their respective meetings.

In the meantime, we would love to hear back from you! Do send us your ideas to make the Interconnect more interactive. Also, do invite your friends to join ISODA. And get covered!

Cheers!

Exclusive "Paid Promotion" offer for ISODA members. ISODA Interconnect now accepts Advertisements/ Paid Promotions from members at introductory prices.

For more information pls reach us at rmgr@isoda.in

Prices as follows:

Quarter Page 125-150 words INR 5,000	Half Page 250-300 words INR 10,000	Full Page 500-600 words INR 20,000

News & Events

Regional Update - West
Date : 13.10.2017

West Regional Meet

Agenda :

- To welcome our community, sponsors and prospects

- Internal Meeting

- Sponsor presentation - Shivaami

- Sponsor presentation - Clear-tax

- Vote of thanks

- Cocktails & dinner

○ It was the first Regional Meet after the AGM and we had 2 sponsors this time. The topics covered by both sponsors was well received.

○ Issues with pricing of Adobe were discussed and it was decided that ISODA would strongly represent all partners with them

○ It was decided to have a gathering for Christmas with family so that the camaraderie amongst the community would increase further.

○ It was discussed that venue for Regional Meeting should be kept more centrally for all to access better, especially since the Metro construction has resulted in a lot of traffic snarls.

West Regional Meet

Regional Update - South
Date : 21.09.2017

South Regional Meet

Agenda :

- To welcome our community, sponsors and prospects

- Internal Meeting

- Sponsor presentation - Shivaami

- Sponsor presentation - Clear-tax

- Vote of thanks

- Cocktails & dinner

The first South Regional Meet for the year was held on 21st September. Mr. N. K. Mehta welcome the members and gave a summary of last year's activities. The progress of Bangalore Chapter initiation was discussed, and membership drive initiatives was discussed. A session on Corporate Story Telling was conducted with the help of an external speaker. The session was concluded with Vote of Thanks by Kabilan.

In conversation with Mr. Ashok Kumar from RAH Infotech, seeking insights on the management of large distribution organization.

1. How you are able to manage a large distribution organization?

As the business grows so does the team size and it is critical to hire the right talent at every level. Hiring the right talent with right skillsets particularly the top management has helped us manage the exponential growth RAH Infotech is witnessing and also remain focused on our core values. It is also very essential to understand what not to do in distribution as this determines which way your growth chart is headed.

Mr. Ashok Kumar
MD & CEO at RAH Infotech

2. What's your success mantra?

Focus, dedications and most importantly, right speed in right direction.

3. What should future distributors look at before starting their business?

With the increased competition in the distribution domain, the margins are getting thinner, finding the right talent is getting tougher and the running costs are on the rise making it a risky proportion. Moreover, managing and balancing between the OEM and channel partner expectation is a key skill good to possess before venturing into distribution domain.

4. What is it that you do to change the perception of customers, partners and vendors to make them take you as serious technology company?

In a fiercely competent domain like distribution, introducing new and advanced technologies that make huge positive impact to customers' infrastructure and enable partners to get additional margins has helped us create a niche for ourselves. This certainly has changed the perception of all stakeholders including OEMs who now consider us as a business partner and not just another box pusher.

Mr. Muneer Ahmed
DigitalTrack Solutions Pvt Ltd

Recognizing Ransomware in the Modern Threat Landscape

The rise of ransomware over the past few years is an ever-growing problem that has quickly become an extremely lucrative criminal enterprise. Targeted organizations often believe that paying the ransom is the most cost-effective way to get their data back — and, unfortunately, this may be true.

Ransomware must be prevented when possible, detected when it attempts to breach a network, and contained to limit potential damage when it infects systems and endpoints. Ransomware defense calls for a "new best-of-breed" architectural approach that spans the organization at the edge in the domain name system (DNS) layer to the data center and across endpoint devices no matter where they're being used.

Ransomware is not a new threat. The earliest known ransomware, known as PC Cyborg, was unleashed in 1989. Since that time, ransomware has evolved and become far more sophisticated.

Despite sensational media reports about massive data breaches targeting organizations and enterprises such as the U.S. Office of Personnel Management (OPM), Anthem Blue Cross Blue Shield, Target, and Home Depot, for identity theft and credit card fraud purposes, the rise of ransomware has become one of the most pervasive threats to organizations and enterprises — as well as individuals — over the past year.

Implementing Best Practices to Reduce Ransomware Risks

There are, of course, a number of best practices that organizations can proactively implement before they're ever targeted by an attacker. If attackers can't easily establish an initial foothold — get their foot in the door, so to speak — they'll likely seek an easier victim, unless your organization is the object of a targeted attack.

So, preventing an attacker from gaining entry to your network with an architectural approach is the most effective way to break the "cyber kill chain" and prevent a ransomware attack from succeeding in the first place.

The following best practices should be implemented to prevent attackers from gaining access to your organization's network and systems:

- Conduct regular security awareness and training for your end users. This training should be engaging and contain the latest information on security threats and tactics.

- Perform ongoing risk assessments to identify any security weaknesses and vulnerabilities in your organization, and address any threat exposures to reduce risk

Unfortunately, despite your best efforts, people are people and there will always be zeroday threats that exploit previously unknown — and therefore, unpatched — vulnerabilities. If an attacker succeeds in accessing your network, his next step is to establish C2 communications. To mitigate the effects of a successful intrusion, implement the following best practices:

- Deploy domain name system (DNS) layer protection that enables you to predictively identify malicious domains, IP addresses, and Internet infrastructure to help mitigate the risk of an attack.

- Automatically enable firewall, advanced malware protection, encryption, and data loss prevention on all endpoints, including personal mobile devices and removable media that is transparent to the user and requires no action by the user. This protects roaming and remote users both on and off the network, even when they don't necessarily do what they're supposed to do with regard to best practices and established policies.

- Enable security functionality on email gateways including blocking or removing executables and other potentially malicious attachments, sender policy framework (SPF) verification to mitigate email spoofing, and email throttling (or "graylisting") to rate-limit potential spam emails.

- Enable security products and services that analyze Internet traffic, emails, and files to prevent infection and data exfiltration and leverage threat intelligence services for deeper context and rapid investigation.

- Design and deploy a robust, inherently secure security architecture that uses segmentation to restrict an attacker's lateral movement in your environment. Enforce the principle of least privilege and eliminate user "privilege creep" to limit an attacker's ability to escalate privileges.

- Regularly back up critical systems and data, and periodically test backups to ensure they can be restored and are good. Also encrypt your backups and maintain them offline or on a separate backup network.

- Assess and practice your incident response capabilities, and monitor and measure the overall effectiveness of your security posture on an ongoing and continual basis.

Most ransomware relies on a robust C2 communications infrastructure, for example, to transmit encryption keys and payment messages. By preventing an attacker from connecting with ransomware that has infected its network, an organization can stop a successful ransomware attack.

About DigitalTrack Solutions

With this ever-growing challenge, organisations are implementing various technologies to ensure that their business is agile to meet the growing demands of their customers. The decision to partner with a solution provider who understands these challenges, architects the most suitable solution and seamlessly integrate the solution with the existing Infrastructure becomes crucial in a dynamic digital environment.

DigitalTrack Solutions Pvt Ltd fits in to this partnership with ease. With more than a decade of experience in managing the challenges in the IT infrastructure, Network & Information Security Infrastructure and Data Management & Availability domains, DigitalTrack is your natural partner. After all, If the Data Matters Partner Matters!

Something's COOKING! Watch this space for MORE!