Great feedback by everyone. In an industry where many companies have outsourced IT requirements to MSP’s and look to them for support and guidance, the need to invest in Cyber Security should be focused in this area so that you do not have a ripple effect where stakeholders, investors, suppliers and clients get affect by a Ransomware, Malware or Phishing attack.

MSP’s need to be protected on a higher level than what people think because they are the bridge for attackers. (Yehudah Sunshine, 2021) As the human factor is the problem with many breaches, education is the first step. If MSP’s start by educating their staff and in turn educate suppliers and the chain, awareness will greatly help people understand the dangers of phishing attacks or clicking on links in an email.

End users do not like to be told about things they need to do to enhance security but recently companies have started using games to educate users on Cyber Security. (Benjamin D.Cone, Cynthia E.Irvine, Michael F.Thompson, Thuy D.Nguyen)

MSP’s should look at engaging in penetration testing so that they can identify any issues and have them addressed. This does not make the MSP value any less but might enhance the relationships with the supply chain because they can report that a number of security issues have been identified and based on the report from the Red Team or Red Shift Team, the issues have been addressed. (J. P. McDermott, 2001)

MSP’s could in turn work with the supply chain and offer the service to supply chain and in turn if everyone has addressed any issues identified, this would put the MSP in a stronger position and relationships will also improve.

To conclude, education is a key factor in fighting Cyber Security. People that are aware of the risks would most likely ask a question first before clicking that link or making a payment to the attacker from a phishing email.

References

Yehudah Sunshine, 2021. *The rise of MSP & CSP vulnerabilities: storehouses for secure data*. Available from:  [**https://www.sciencedirect.com/science/article/abs/pii/S1361372321000208**](https://www.sciencedirect.com/science/article/abs/pii/S1361372321000208) [Accessed 30 August 2021]

Benjamin D.Cone. Cynthia E.Irvine. Michael F.Thompson. Thuy D.Nguyen. 2007. *Attack net penetration testing*. Available from: [**https://www.sciencedirect.com/science/article/pii/S0167404806001556**](https://www.sciencedirect.com/science/article/pii/S0167404806001556) [Accessed 30 August 2021]

J. P. McDermott., 2001*. Attack net penetration testing*. Available from: [**https://dl.acm.org/doi/abs/10.1145/366173.366183**](https://dl.acm.org/doi/abs/10.1145/366173.366183) [Accessed 30 August 2021]