RSA Conference 2021
COVID & the Expanded Attack Surface

RSAC Virtual 2021 kicked off on Monday May 17th with a keynote titled "A Resilient Journey" from Rohit Ghai, RSA's CEO. Unsurprisingly, one of the big themes of the keynote was how COVID-19 forced IT and IT security to rethink how we approach remote workers, trust, resiliency, and hacks when most of the workforce of a variety of companies were forced to work remotely. BYOD (bring your own device) went from being an interesting (and sometimes painful) use case to one that was the overwhelmingly common use case for employees. We also went from in-person meetings to "Zoom everywhere".

These changes radically expanded the attack surface that cybercriminals and malicious state actors could (and did) try to exploit in 2020-2021, with results including the SolarWinds Hack (Dec 2020), the Colonial Pipeline hack (May 2021), Microsoft Exchange hacks (March 2021), and a variety of other attacks. Rohit also stated that there is an equal number of attacks that were prevented or mitigated, including the FBI's "cleaning" of Exchange Servers in April, the US elections (largely without issue), and the stopping in February 2020 of the largest DDOS attack to date.

What we have learned to date in these new times:

- “Zero Trust” and “100% authentication” is morphing into continuous authentication – looking not only at credentials, but user activity and behavior throughout their presence on IT resources, and not just at login.
- Sharing information across organizations is critical to identifying issues (essentially how the SolarWinds hack was exposed).
- Third-party/fourth-party risk management is a real issue, as illustrated by the SolarWinds hack, which showed how supply chains and vendors to our vendors can be exploited by hackers.

Mike Heumann, Managing Partner

G2M Communications, a re-grate-it inc. brand