Q. How has the attitude of cybersecurity changed over the past few years?

A. It has become a board room topic and a kitchen table topic and every point across that spectrum. Consumers/citizens have become much more aware and sensitive to risks. Organizations are made up of consumers/citizens. The regulatory environment is a driver globally. The global pandemic has pushed just about everything online that can go online.

Q. Where does the industry stand now in terms of preparedness, in your opinion?

A. As attitudes toward cyber risk and data privacy have shifted rapidly in the past few years, demonstrated digital trustworthiness is becoming a differentiator in the market. The costs associated with cyber risks has been on a strong growth curve and is driving regulations globally. Industries do not move as quickly as the marketplaces has been moving.

Q. Do you see cybersecurity as an opportunity for integrators (i.e. RMR or recurring monthly revenue)

A. Lifecycle management services such as maintenance, patching, tuning, assessment of security posture, etc. Designing in the ability to use installation telemetry to proactively identify opportunities to maintain the strongest possible security posture across the lifecycle of an installation.

Q. Are there any common weaknesses when dealing with cybersecurity within access control?

A. Unsecured network traffic, the use of network segmentation when on enterprise networks, maintaining up to date firmware and software across all elements of the ecosystem, to name a few.

Q. What resources can you recommend to become more knowledgeable on cybersecurity? Are there any events or trainings I should pay attention to or possibly attend to become more cyber aware?

A. There are myriad of sources. Pick a sub-topic and dig into it with the industry experts in those specific disciplines (i.e. software development, cloud operations, network security, identity and access management, etc.)

Q. What is the role of the security manufacturer in cybersecurity?

A. Make digitally trustworthy devices and solutions and ensure effective maintenance and upkeep across the lifecycle of those devices and solutions. Also, to be mindful of interoperation with other components or systems.

Q. Where do I start with cybersecurity planning?

A. Cybersecurity programs must align to the current business and threat environments.

- What are you protecting for the business in question?
- What threats are the business facing?
- What is the current state of the organization's security posture relative to the current threat landscape in which the operates?
- Prioritization will be required as an organization invests in growing its cybersecurity maturity across all functions and process areas.

Q. What are the minimum level discussions I should be having with my End User Customers concerning cybersecurity?

A. Bring the customers' requirements and expectations to the surface so there are no assumptions or guessing. Cybersecurity has value. Customers must be clear about the risks they are willing to accept versus the ongoing costs of cybersecurity. Gauge customer awareness of cybersecurity and help them grow their knowledge and appreciate of what cybersecurity means to them and the things they care to protect.

Q. Tell us more about the notion of "Digital Trustworthiness"

A. Key concepts:

- "Digital trust is the confidence users have in the ability of people, technology and processes to create a secure digital world…
- Digital trust is given to companies who have shown their users they can provide safety, privacy, security, reliability, and data ethics with their online programs or devices…
- Digital trust will allow customers to find and choose the dependable digital services faster, better and with less unreliable choices to distract them…
- Eventually, machines will automate the decision process by calculating the level of confidence in a program.
- This will require more information to be provided about a company's service or product, creating increased transparency that will also build digital trust."
- References:
  - https://whatis.techtarget.com/definition/digital-trust
  - https://cybersecurity.att.com/blogs/security-essentials/digital-trust

Q. Do you have a best practice checklist for security installations?

A. Checklists can be helpful tools to ensure we think broadly and consistently. However, we should be mindful not to be overly reliant on checklists and follow them exclusively. If one has repeated patterns of work or standard installation processes, checklist can be very valuable. Be mindful of exceptions as no two installations are exactly alike.

Q. Cyber security and physical security are getting closer and closer. Do you see the industry merging together anytime soon? If so, what do an integrator should do to have a cyber security program in place?

A. Currently we are seeing the physical security and physical security getting closer and closer. In some circles they have merged. For an integrator, have a cyber security program in place will be required. The first step in that endeavor will be to educate yourself on cyber security topics.

Q. A listener was part of a recent presentation in which that presenter commented that security devices were the primary method into a network for a hacker, what are some basic but effective practices an installer should follow? Remember they are not IT professionals.

A. Some basic things that can be done is to ensure security devices are isolated on their network with network segmentation and default password should be changed. There are many other items that can be done to secure the device, but protection is only one portion that needs to be done. Remember, PROTECT – DETECT – CORRECT.

Q. Any best practice for "Ransom" attacks similar to what just happened to Garmin?

A. Ransom attacks or ransomware are growing in both frequency and impact. The evolution of ransom attacks have gone from smaller scale, lower fees to large-scale and expensive – sometimes over $1M USD. Sound network and endpoint protections can thwart many of these types of attacks. Coupled with effective backup and recovery methods for critical data, one can have an effective approach to avoiding and recovering from ransomware. The FBI's current stance on whether or not to pay a ransom is to avoid it if possible since in the end, payment only incents more attacks and funds organized crime.