Current Risk Management Practices:

1. The great challenges are:
    a. Organizational Politics/Culture – Organizations or management not willing to assess their security posture for critical infrastructure because of potential career suicide.
    b. Device Resiliency – Certain critical infrastructure lacks resiliency to be tested all out without breaking the device.
    c. Laws – as new legislation is written to prosecute criminal cyber activity, the laws put cybersecurity researchers and cybersecurity practitioners in unusual situations where their ability to their jobs without breaking laws.
2. The biggest challenge in open cross sector standards are the willingness to share information and share challenges each industry sector is facing.
3. Our organization philosophy centers on the concept that a security incident is occurring whether we detect it nor not. Senior management defines the framework, and derives all security and risk management input from all levels.
4. Our organization locates our cybersecurity risk management program with management.
5. We regularly perform weekly security assessments, both announced and unannounced, on all our infrastructure. Our definition and risk management is based on the volume and value of information to our organization. The value and volume of information generally corresponds to our business continuity/disaster recovery where on areas we value information and how we protect the information.
6. Cybersecurity risk is incorporated by default into our enterprise risk management. It is a integral part and its inception and integration happens at the beginning. From software development to information system requirements, we strive to incorporate technology and software that is highly resilient to attacks.
7. We use an in-house proprietary best practice method centering on defense in depth and high levels of resilient applications and technologies.
8. Reporting requirements are not uniform, and brings challenges when it comes to different groups or agencies.
9. Any device touching a computer network or the internet by any communication method is considered interdependent.
10. Decline to comment.
11. Not Applicable.

General Thoughts as questions

The biggest challenge and overall thought process is that cybersecurity needs to be adopted as a whole. Security is not meant to be selected like a pair of shoes or a loaf of bread. Cybersecurity is a holistic approach where every component is interdependent. A failure of one interdependency currently may bring down an entire group. While we attempt to compartmentalize security incidents, security posturing for most organizations is not mature enough to execute such an objective.

The most critical issues stand right now are:

- Device and Software Resiliency – Existing programmers and technology being pushed to the market are not resilient to a security attack. The mentality programmers are taking is one of "they will never attack this device" or "it will never happen". Programmers must adopted a mentality that security incident will occur and when it does occur, a device can survive such an attack, even if it is a simulated attack designed to assess its ability to survive such an attack.
- Culture – Organizations are not adopting the cybersecurity culture. Management is not adopting the cybersecurity culture. The mentality is always one of "it will never happen to us" or "why would anyone want to attack us?".
- Testing and Training – We need to have safe controlled environments to train, test, and examine patterns and security issues. We need to have much better access and communications across all industry lines. We need to be able to generate attack based traffic with an expected set of results, and be able to guide investigators and defenders to identify those patterns and understand what they are seeing. It is one thing to train people to know something. It is another to recognize, understand, and comprehend that same body of knowledge.
- Holistic approach – security must be designed into all aspects of technology. From the process to developing the hardware, the software, the firmware. It must be tested, retested, and tested again to ensure the quality. Regulations should be in place to encourage the adoption of best security practices.
- Incident Now, not later – Far too many organizations are adopting the security posture of it isn't happening and are never at a state of readiness. When an incident does happen, the ability to move from an idle to a state of readiness requires so much resources and time that an incident has happened, and organizations have suffered great losses. Organizations need to be at a ready state consistently to defend and protect their digital environments.