The number of successful cyber attacks in the U.S. has grown 144 percent in the past four years, and the rest of the world is close behind. In that same time, the cost to the average company has almost doubled. On average, advanced attacks now persist in the network seven months before they are detected. And the time to resolve those attacks once detected has increased by 221 percent to 45 days. Victims suffer financial losses, damage to brand, and damage to customer relationships.

Answer the following questions to get a better understanding of how prepared your organization is in case of a cyber attack.

Do you perform a periodic cybersecurity focused risk assessment?
- Have identified (ie. inventoried) the types of data you store that could be exposed during a data breach?
- Do you estimate the cost of recovery of your crown jewels (data) if stolen?
- Do you consider cyber insurance?
- Do you establish priorities for protection and recovery?
- Do you know where your PII (Personally Identifiable Information) and PHI (Personal Health Information) data are stored?
- Do you adequately protect them?
- Do you mitigate the risk?

Have you developed an enterprise security plan?
- Do you have adequate investments made in securing technologies and physical locations?
- Have you assessed the effectiveness of the technology to detect threats?
- Are you prepared to respond to a data breach?
- Are both stakeholders and functional experts engaged?
- Is your plan aligned with your budget?
- Do you review and update it at least annually?
- Have you identified third-party vendors contracts to engage in the case of a data breach?

Do you have the right team in place?
- Do you have a good understanding of the skills needed?
- Qualified, certified enterprise security professionals are in demand – how do you recruit them? And more importantly, are you able to retain them?
- Does your team’s experience cover a wide spectrum like mobile, cloud, application security, video, platform, etc.?

What functions and technologies have you deployed to protect your organization?
- Have you designed your defense to be deployed in layers since no single cyber defense is 100% effective?
- Do you have a “strong/enhanced” password culture?
- Are you able to erase data on devices that are stolen?
- Do you encrypt your data on your workstations, laptops, mobile devices and backups?
- Do you perform regular penetration testing and vulnerability scans? What corrective actions are taken based on these reports?
- Do you have the technologies and processes in place to conduct a thorough forensic investigation into a cyber security incident?
- Do you have the platforms/technologies to collect data with reference to threat intelligence from your environment?

How do you keep your employees informed and up-to-date with respect to cybersecurity?
- Have you conducted employee training to apply security best practices in the last 12 months?
- Do you know that over 60% of the data breach incidents are on account of insiders (employees, consultants, contractors, etc.)?
- Are you aware that security (including cybersecurity) is one of every employee’s top priorities?
- Have you developed a communications incident response plan including drafts of key media materials that will be useful during an incident (e.g., statements and Q&A)?
- Do you have media-trained spokespeople and executives specifically on security matters?