CGI | GOVERNING INSTITUTE

September 2015

Can you answer the following 10 questions about the state of your organization's cyber readiness?

1) What is my role in the cybersecurity efforts of my organization?
2) Has my organization adopted the NIST Cybersecurity Framework?
3) How are cybersecurity activities funded in my organization?
4) Do we have a strong cybersecurity team and a plan to deal with the market's shortage of cybersecurity talent?
5) Do we have an up-to-date breach response plan?
6) Do we have an executive dashboard that helps us know when and why to make cyber investments?
7) What agencies and departments are at the highest risk of an attack or breach?
8) Do we require regular cyber-awareness training for our employees?
9) Are we communicating with critical infrastructure organizations to ensure economic viability?
10) Are we constantly communicating with stakeholders, including constituents, about the likelihood of a breach and how to be prepared?

If the answer to any of these questions is no, then Governing Institute and CGI — a leading IT and business process services provider — invite you to read, "Guide to Cybersecurity as Risk Management: The Role of Elected Officials." This timely guide offers checklists of the top cybersecurity action items for elected and agency executives and lawmakers; an overview of public sector threats, assets and adversaries; and in-depth recommendations for integrating cybersecurity into an organization's risk management framework.

For a complimentary PDF, download the guide at: www.governing.com/cybersecurity-guide

Sincerely,

Todd Sander
Vice President of Research
e.Republic

Molly O'Neill
Vice President and U.S. State and Local National Executive
CGI