CYBER

Cybersecurity Survey

Section One: Qualifying Questions

1. **Please select the category that best represents the total gross sales or revenues for your corporation, firm, or organization in 2015. (Please include all plants, divisions, branches, and subsidiaries in all countries.)**
   __ Less than $20 million
   __ $20 million to $249 million
   __ $250 million to $499 million
   __ $500 million to $999 million
   __ $1 billion to $4.9 billion
   __ $5 billion to $9.9 billion
   __ $10 billion or more

2. **What is your current title or position?**
   __ CEO / President / Chairman / Owner
   __ C-level Executive (e.g., COO, CFO, CMO, CIO, etc.)
   __ Upper management but not C-level (e.g., Sr. VP, VP, Director, etc.)
   __ Mid-level management (e.g., Manager, Account Executive, etc.)
   __ Technical / Scientific (e.g., IT, Programmer, Engineer, Scientist, etc.)
   __ Other _____

3. **Which of the following best describes your company's industry? (If more than one, please select the industry that accounts for the largest share of your company's revenue.)**
   __ Aerospace / Defense
   __ Agriculture / Forestry / Lumber
   __ Architecture / Construction
   __ Automotive
   __ Banking / Financial Services / Insurance
   __ Business Services (e.g., advertising, staffing, etc.)
   __ Chemicals / Adhesives / Paints / Plastics
   __ Clothing / Outerwear / Footwear / Textiles
   __ Consulting / Professional Services / Accounting Services / Legal Services
   __ Consumer Products (aside from food, beverages, clothing, electronic products)
   __ Education / Training
   __ Electronic Products, Computer Hardware
   __ Food / Beverage Products
   __ Health Care / Medical Services
   __ Hospitality / Restaurants / Hotels / Leisure Attractions
   __ Industrial Equipment / Machinery / Instruments
   __ Natural Resources (e.g., mining, metals, energy, cement, etc.)
   __ Non-Profit / Charity / Religious Organization / NGO
   __ Pharmaceuticals / Biotechnology / Medical Devices
   __ Publishing / Printing / Broadcasting / Media / Journalism
   __ Real Estate / Property Management
   __ Retail Stores / Retail Sales
   __ Software
   __ Technical / Scientific Services / IT services
   __ Transportation / Logistics / Distribution / Shipping
   __ Utility (e.g., cable, electricity, natural gas, telephone, water, etc.)
   __ Other: _____

Section Two: Multiple Choice Questions

1. **To perform your leadership role, do you feel it is important for you to understand the nature of cyber threats?**
   __ Yes
   __ No

2. **Do you feel that you have a sufficient understanding of cyber threats relative to your role?**
   __ Yes
   __ No

3. **Of the various forms of damage a cyber incident can cause, please indicate the form of potential damage to your organization that concerns you the most, second most, and third most:**

	Most	2nd Most	3rd Most
Degradation of customer loyalty	__	__	__
Degradation of our brand and reputation	__	__	__
Loss of revenue	__	__	__
Loss/theft of intellectual property, proprietary info	__	__	__
Disruption of critical business processes	__	__	__
Damage to equipment and/or data	__	__	__
Regulatory actions or sanctions	__	__	__
Other (specify): _____	__	__	__

4. **If your organization were to experience a major cyber incident, which of the following would be the most, second most, and third most costly to your organization by the time you have done everything needed to handle the incident?**

	Most	2nd Most	3rd Most
Regulatory defense or regulatory fines	__	__	__
Legal fees and settlements	__	__	__
Forensics services	__	__	__
External incident response support	__	__	__
Customer notification and monitoring costs	__	__	__
Public relations	__	__	__
Data recovery services	__	__	__
Services to recover IT infrastructure	__	__	__
Services to recover business operations	__	__	__

5. **Do your technology leaders provide business leaders with regular reports on the security posture of the organization?**
   __ No, there is no security reporting process
   __ Yes, reports are provided on at least a weekly basis
   __ Yes, reports are provided on at least a monthly basis
   __ Yes, reports are provided on at least a quarterly basis
   __ Yes, I have continuous access to a security or cyber risk dashboard

6. **When your organization undertakes a strategic business initiative, which of the following best describes how security and cyber risk concerns are addressed?**
   __ Most of our strategic business initiatives do not have security or cyber risk concerns associated with them
   __ Sometimes security or cyber risk concerns are raised during the planning process
   __ It is a routine part of our planning process to identify and address security and cyber risk concerns
   __ We address security or cyber risk issues if they arise after a strategic business initiative has been executed

7. **Did you (or do you) provide input or consultation in the design of the cyber incident response plan?**
   __ Yes, I had/have been consulted during the design of the plan
   __ Yes, but I was asked to review the plan only after it was drafted
   __ No, but I was informed of the plan
   __ No, I have not been involved in any way
   __ We do not have a cyber incident response plan

8. **Has the cyber incident response plan been rehearsed within your company?**
   __ Yes, and I have been involved in rehearsals
   __ Yes, but rehearsal activity does not involve me
   __ No   __ Don't know   __ We don't have a plan

9. **Do you have a clear understanding of the tasks and functions that may be required of you and your team if a major cyber incident occurs?**
   __ Yes, I am reasonably confident that I will be able to contribute effectively
   __ To some extent, but I do not feel we are sufficiently prepared
   __ No, there is significant room to improve my knowledge in this area
   __ Not applicable to me / others would have all of the responsibility for addressing a major cyber incident
   __ Other (specify): _____

10. **Has your organization been the victim of a cyber incident in the past two years that has received executive attention within your organization?**
    __ Yes   __ No   __ Prefer not to say

11. **Has your organization ever been the victim of a cyber incident that has received executive attention within your organization?**
    __ Yes   __ No   __ Prefer not to say

Section Three: Qualitative Questions

I. **In your opinion, where should your company be focusing more effort to improve overall cyber risk posture?**

2. **What is the most effective thing your organization has done in the past year to improve cyber risk posture?**

Please visit this survey online at leadersmag.com/cybersecurity.