










CYBERSECURITY QUIZ



Rate the following cybersecurity statements as “True” or “False.” Try to answer to the best of your knowledge without checking the answers on page 2. **READY, GET SET, GO!**

CYBERSECURITY STATEMENTS		TRUE	FALSE
1	 Small businesses are safe from cyber attack(s).	<input type="radio"/>	<input type="radio"/>
2	 When making an investment in cybersecurity , you should consider: a) the value of the data, b) the probability it can be breached, AND c) the effectiveness or “bang for your buck” that the new control provides.	<input type="radio"/>	<input type="radio"/>
3	 Over 90% of successful cyberattacks start as phishing emails.	<input type="radio"/>	<input type="radio"/>
4	 If stolen credentials resulted in a substantial loss from your business banking accounts, the bank would be responsible to cover the loss.	<input type="radio"/>	<input type="radio"/>
5	 There is a limit beyond which investing in cybersecurity is not worth it.	<input type="radio"/>	<input type="radio"/>
6	 If a block of data is stolen from your business, such as customer information, the first thing you should do is notify those affected.	<input type="radio"/>	<input type="radio"/>
7	 The most cost effective approach to cybersecurity is to protect the information that is most vulnerable to attack.	<input type="radio"/>	<input type="radio"/>

BBB CYBERSECURITY QUIZ ANSWERS

Now tally up your results against the answer sheet and find out how many questions you've answered correctly. For each correct answer, give yourself a point.



CYBER \$3CURITYSM

1



FALSE

More than one out of five small businesses reported being the target of a cyber attack.

Approximately one out of five small businesses expect to lose money to a cyber attack in the next 12 months. And only 35% of businesses could remain profitable for three or more months if they permanently lost access to essential data.

87% OF RESPONDENTS ANSWERED CORRECTLY

2



TRUE

A simplified and adapted version of the Gordon and Loeb model can be summarized in five steps.*

1. For each information set in your organization, estimate the potential loss that you could incur in a cybersecurity breach.
2. Estimate the probability of a cyber breach for each information set.

85% OF RESPONDENTS ANSWERED CORRECTLY

3. Identify the potential investments that you could make in cybersecurity.
4. Estimate the reduction in the probability of a cyber breach due to the additional investment.
5. Compare the investment cost to the potential savings. As long as the potential savings exceeds the cost of investment, then it is a cost-effective measure that should be implemented.

3



TRUE

Only one employee needs to click on a bad link in an email or open an infected attachment for an attack to get in the door of a business. The risk that an organization will be successfully attacked through email is directly proportional to the number of employees.

79% OF RESPONDENTS ANSWERED CORRECTLY

4



FALSE

The burden of proof lies with businesses – not banks – when it comes to cyber incidents on accounts used for commercial transactions.

50% OF RESPONDENTS ANSWERED CORRECTLY

5



TRUE

Per the Gordon and Loeb Framework to Assess Cost Effectiveness of Cybersecurity **there is a point where a dollar invested in cybersecurity results in less than a dollar's worth of protection.**

42% OF RESPONDENTS ANSWERED CORRECTLY

6



FALSE

Ideally, all businesses should put a plan in place before a breach occurs as part of advanced incident response planning. Consulting and following that plan should be the first step if data is stolen from the business. Notifying those affected will be early in that plan, but consulting your legal counsel usually comes first.

20% OF RESPONDENTS ANSWERED CORRECTLY

7



FALSE

While protecting your most vulnerable data is often the correct approach, **many times the value of the data does not justify the expense.**

17% OF RESPONDENTS ANSWERED CORRECTLY

TOTAL SCORE OUT OF 7



In spite of respondents' general awareness of cybersecurity risks, there are still opportunities to better educate smaller businesses on the topic and dispel cybersecurity myths. BBB's Cybersecurity Program aims to assist smaller businesses with the knowledge and resources needed to be cyber secure. Please feel free to share with friends and the business community.

*<http://www.scirp.org/journal/PaperInformation.aspx?paperID=64892>