The Most Comprehensive Questions You Can Ask Yourself

to See if Your Company is Prepared for a Cyberattack

The Most Comprehensive Questions You Can Ask Yourself to See if Your Company is Prepared for a Cyberattack

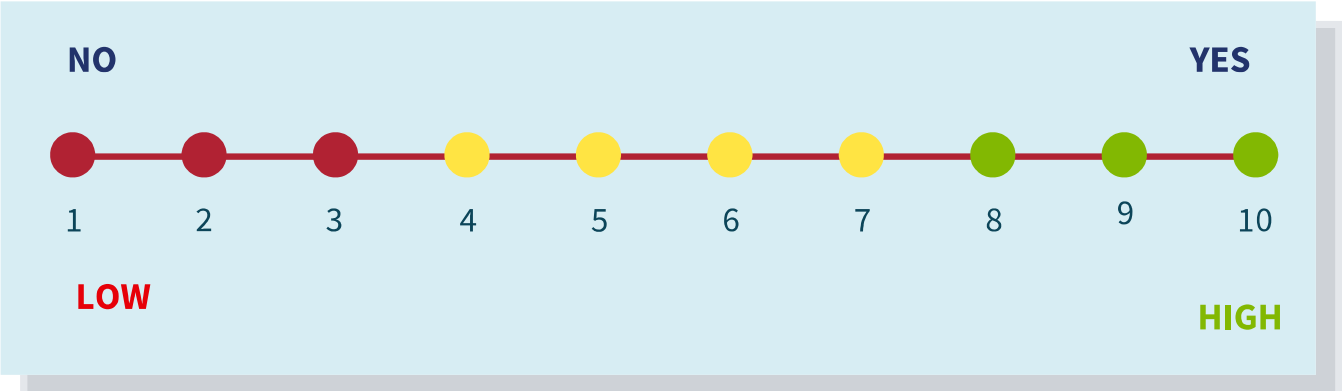
This simple survey is meant to get you thinking about a complex topic: **cybersecurity.**

Take this survey to test key elements of your preparedness. It is intended to point out important elements of your cybersecurity strategy and its implementation.

Your responses to the questions are either a relative score from 0 to 10 (0 = least prepared to 10 = most prepared) or a yes/no answer with a no being 0 and a yes being 10 (or select a number based on your relative preparedness).

Calculate your average score to get an overall sense of your cybersecurity preparedness.

LEVEL OF PREPAREDNESS



GOOD LUCK!

01 How confident are you in your organization's overall security posture?

02 How would you rate your organization's overall cybersecurity strength (ability to resist cyberthreats)?

03 Has your organization been compromised by a successful cyberattack one or more times within the past 12 months?

04 How difficult is it to detect and prevent insider attacks compared to external cyberattacks?

05 Are you satisfied with the amount of time it took for your organization to recover from a cyberattack (on average)?

06 Can you quantify the negative impact the security incidents had on your company in the past 12 months?

07 What is the likelihood that your organization will become compromised by a successful cyberattack in the next 12 months?

08 Are your cybersecurity strategies aligned with your business and operational goals?

09 Do your cybersecurity metrics relate to business risk and business objectives?

10 Are your cybersecurity objectives quantified and measured?

11 Do you provide oversight to such measurement?

12 Do you have a complete picture of your attack surface?

13 Are you certain you are not blind to some risks and vulnerabilities?

14 What is your level of certainty of which privacy regulations and laws your organization has to comply with?

15 Are you confident that you are fully compliant with those you know about?

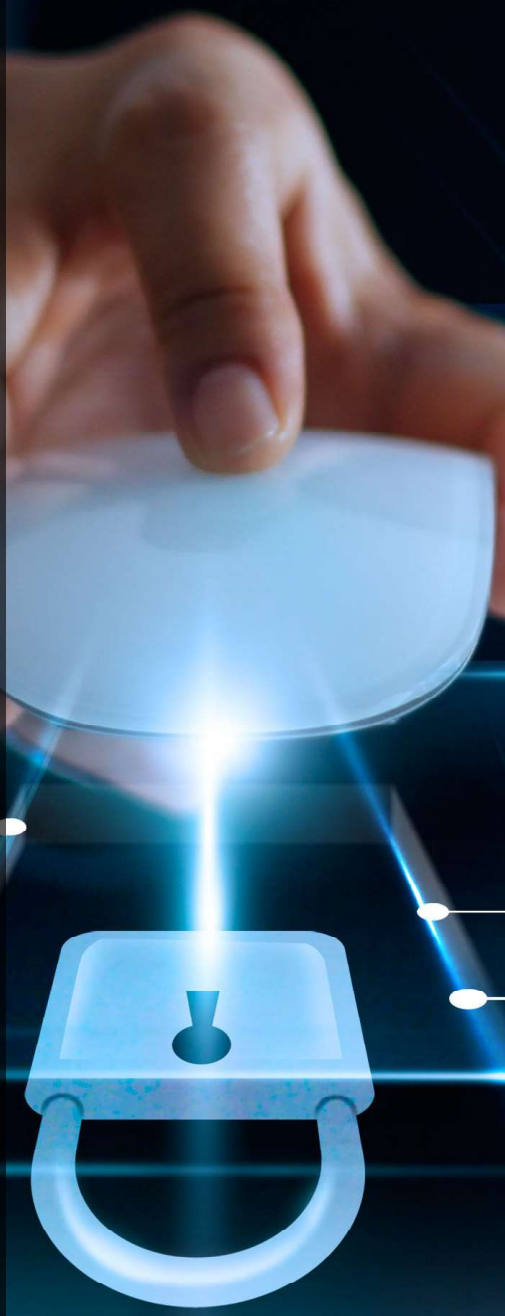
16 Have you measured the maturity of your cybersecurity strategy?

17 Have you benchmarked your cybersecurity strategy to analyze the extent to which each practice is performed?

18 Do your security audits and risk assessments identify critical gaps that show where you have vulnerabilities?

19 Is your Cybersecurity Governance framework based on international standards and best practice?

20 Do you feel there is adequate investment in cybersecurity in your organization?



21 Have you developed one or more business cases to motivate the investment required to protect the organization's information assets and to increase business resilience?

22 Do you have a portfolio of work to realize the requirements identified in the strategy, motivating the investment in developing & deploying required solutions, and aligning the organization and its expectations to the work portfolio?

23 Have you identified which types of sensitive data you are most concerned about protecting (for example, email, customer data, sales & marketing data, intellectual property (designs, formulas, blueprints), and so on)?

24 Have you identified which barriers inhibit your organization from adequately defending against cyberthreats (for example, low security awareness among employees, lack of skilled personnel, lack of budget, poor integration / interoperability between security solutions, and so on)?

25 Do you have a documented plan that describes your response to a cybersecurity attack?

26 Have you successfully tested the plan?

27 Do all your employees explicitly understand their roles in terms of cybersecurity?

28 Have you planned for key man dependency (ie, what if critical resources are unavailable when there is an attack)?

29 Have you identified and understood the needs of every security stakeholder in the organization?

30 Are your line-of-business executives accountable for meeting the cybersecurity objectives?

Since the list is neither comprehensive nor does each question carry the same weight, the score is less important than how you feel after answering all questions.

YOU MAY FIND IT USEFUL TO ASK COLLEAGUES IF THEY HAVE THE SAME OPINION AS YOU DO.

IT IS A MATTER OF WHEN, NOT IF YOUR COMPANY WILL EXPERIENCE A CYBERATTACK

Cybersecurity risk is the probability of experiencing damage or harmful loss of critical assets (sensitive data, finances, or business operations) because of a cyberattack or breach. A cybersecurity risk assessment sets out to understand the existing system and environment, identifies the various information assets that could be affected by a cyberattack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies and quantifies the various risks that could affect those assets.

KNOWLEDGE IS POWER
– THAT IS WHY YOU NEED A CYBERSECURITY RISK ASSESSMENT

It is impossible to combat cybersecurity risks without first understanding where your business is vulnerable. The cybersecurity risk assessment identifies the various information assets that could be affected by a cyberattack (such as hardware, systems, laptops, customer data, and intellectual property). It identifies the associated risks that could affect those assets and evaluates all the known vulnerabilities and determines which vulnerabilities are likely to be exploited as well as the potential for damage to the business.

A cybersecurity risk assessment gives the business the ability to proactively defend themselves from cyberattacks. The key questions that the cybersecurity risk assessment answers are:

1. Where is my business vulnerable?
2. How would a cyberattack impact my business?
3. How do I fix the vulnerability?
4. How do I recover from a cyberattack?
5. How can I limit the damage?

If you can answer these questions, you can determine what to protect. This means you can develop IT security controls and data security strategies to mitigate risk.

A top-down risk assessment will highlight how prepared you really are, what steps you can take to increase your preparedness, and ultimately enable you to get peace of mind that you are at low risk of having an attack, and should an attack occur, you can work your way through it with least impact to your operations and reputation.

NOT ALL APPROACHES ARE EQUAL

There are numerous approaches and methodologies available to conduct a successful Cybersecurity Risk Assessment. Our approach at CyberConnect Projects is somewhat different. It goes beyond standard approaches in that we acknowledge that most organizations already have both cybersecurity strategies and implementations in place. We analyze these and validate that they are indeed sufficiently robust and effective for your business needs and that they do align with your business objectives.

Our method sets out to identify gaps in the strategy itself (knowing what to do), as well as gaps in the alignment of the strategy to the real implementation (doing what you know). These gaps are often quite subtle. For example, the strategy may indicate the need for a world-class, best-of-breed Privacy Access System (PAS). Such a system may certainly be in place, but issues within the implementation itself may yield risks that business executives don't know about. There is often misalignment between protection that executives believe is in place, and the actual protection really provided, giving the organization a false sense of security.

OUR APPROACH TO A CYBERSECURITY RISK ASSESSMENT

01 IDENTIFY your information assets

We facilitate a series of workshops and interviews with your key cross-functional business managers and IT professionals to determine information such as:

a. What data or information assets do you have, how are they collected, where are they located, what are their attributes, and what is the level of protection each asset has?

b. Which data is valuable to you? Will it cost money to reacquire it? Would there be legal, reputational or financial repercussions if you couldn't provide the data when needed? Would it have an effect on operations if you could not access the data?

c. Is information managed and maintained by the business and/or by external parties?

d. What are the processes by which the data is governed? That is, what are the controls to manage, maintain, measure, protect and dispose of the data?

e. How is the data classified?

02 ANALYZE

your cybersecurity strategy, implementation, and the alignment between them

Strategies are often well constructed, formal documents, but may sometimes be less formal, and incorporated into other business and IT documents. Our tasks include:

a. Check the strategy for comprehensiveness, clarity, and alignment with best practice security standards (for example NIST[1]).

b. What are the threat vectors and data breaches that are most relevant to YOU?

c. Review the risks that have been identified in the context of the current inventory of your information assets and ensure that adequate and appropriate risk assessment and analysis has been applied with respect to probability and impact.

d. What is the timeline to respond to threats and breaches?

e. Who is responsible for defined activities and controls?

f. Confirm that the objectives are both qualitative and quantitative in nature.

g. Review the plan that is followed when a threat is detected, or a vulnerability is exploited (when a cyberattack occurs).

h. Determine whether the strategy addresses all relevant stakeholders, both within and outside of the organization, whether their roles and responsibilities are clearly defined and practiced, and examine whether communication is adequate and appropriate between all stakeholders, specifically between business- and technology-focused groups.

A good implementation shows that you have 'done what you know'. In a top-down risk assessment of this nature we facilitate a series of workshops and interviews with your key cross-functional managers and IT professionals to:

a. Test whether the essence of the strategy has indeed been implemented.

b. Identify gaps between the strategy and the implementation.

c. Test whether best practice principles are adopted (for example password management, user authentication, privileged access management and so on).

[1] National Institute of Standards and Technology

03 DOCUMENT the findings

Assessing risk is a process rather than a single event. Our high-level top-down risk assessment will collate our findings in a report that will help the company's executives make decisions on whether the current cybersecurity strategy and its implementation is sufficiently robust, comprehensive, and appropriate for their business' threat landscape. The identified gaps will indicate potential steps that should be considered to secure the business better.

This report provides a baseline of your preparedness at a point in time. It gives you and your executives confidence that your organization is indeed on track and prepared for likely threats to occur, and it can highlight potential areas to focus on so that you are continuously improving your preparedness. It provides a means to focus your financial investments wisely.

Once possible risks have been identified, analyzed and documented, safeguards can be put in place to mitigate the likelihood of a cyberattack occurring or limit the damage caused by an attack if it does happen. CyberConnect Projects specializes in protecting your business by assessing your cybersecurity risks and minimizing them.

A good cybersecurity risk assessment can be overwhelming.

HOWEVER, YOU DON'T HAVE TO DO IT YOURSELF.

OUR PRAGMATIC APPROACH IS COMPREHENSIVE AND YIELDS RAPID VALUE TO YOU!

As a thank you for downloading our survey, we would like to offer you a discounted rate on our comprehensive cybersecurity risk assessment.

For only $14,700

We will conduct a cybersecurity risk assessment by reviewing your cybersecurity strategy and implementation, identifying potential gaps, and reporting on your preparedness.

To claim your cybersecurity risk assessment, please contact glenda.wheeler@cyberconnectprojects.com

TERMS AND CONDITIONS

- For this fixed price offer, the depth and breadth of the report will depend on timely accessibility and quality of required information / resources, size and complexity of your business.
- On engaging we will confirm the explicit scope, metrics and deliverables.
- We will agree which of your key cross-functional business managers and IT professionals will participate in the engagement.
- The findings will be based on the information (verbal and written) received from your personnel rather than from our consultants directly accessing your IT systems.
- The engagement will be limited to a 4-week elapsed time period.
- Payment will be 60% at the commencement of the engagement and 40% on delivery of the report.