IS MY COMPANY AT RISK?

A CYBER SECURITY SELF-ASSESSMENT QUESTIONNAIRE

decide

DECIDE WHAT HAPPENS

11211 Katy Freeway Suite 680 Houston, TX 77079
281.596.0123 | DecideConsulting.com | Info@DecideConsulting.com

Why Do You Need a Cyber Security Assessment?

The motivation for cyber hackers is higher now than ever before. This is a threat to businesses small and large. The cyber criminal has more tools at their disposal that can do more harm. Many executives authorize a few cyber defenses and think they are done. Just because your organization was secure a year ago, does not mean you are secure today. The world has changed and new threats exist.

THINK ABOUT THESE FACTS:

- Cyber Attacks are More Profitable than Ever
- Today's Cyber criminals are highly skilled, aggressive and more elusive than ever
- Better hacking tools and increased profit create a highly motivated criminal
- Firewalls, anti-virus and anti-malware are no longer enough
- Companies of all sizes are targets
- SMBs are often the portal to larger companies
- If you put up cyber defenses a year ago, things have changed

About this Cyber Security Self-Assessment

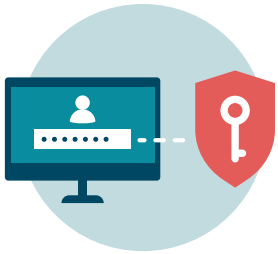
The following Cyber Security Self-Assessment is comprised of 14 sections of no more than 5 questions. Each of the questions are "yes/no"

DIRECTIONS:

For each question, **"check"** for a Yes. Leave the box unchecked for a **"No"**. Each section has a tally table at the bottom that sums the **"Yes"** answers. The total the number of yes answers for each section are totaled on the last page. Your score is the total number of "Yes" answers multiplied by 1.5 Your score should be used to gauge as a statement of cybersecurity readiness.

You may not know a term we are using in a question. Those questions should remain unchecked. There are terms centric to cyber security professionals that have not worked their way to all IT professionals and the C-suite.

While even a perfect score does not guarantee a risk-free environment, the lower the score, the higher the likelihood and greater the impact a cyber-related event will have on brand integrity.



Policy

1. Does this organization use cyber-related policies that are approved by the C-Level? ☐
2. Is there an Acceptable Use and/or other data related policies in effect? ☐
3. Are they well communicated, well understood and is it enforced? ☐
4. Is Training and Awareness a required part of annual certification for all employees? ☐
5. Do you have an Identity Lifecycle Management policy? Do HR and IT each have responsibilities in it? ☐

TOTAL 0

Staff Review

1. Have the roles, responsibilities, expectations and measures for the resources been clearly communicated? ☐
2. Are the members of the IT staff engaged in cybersecurity trained and certified or have they learned mainly from "on the job training"? ☐
3. Are they confident in their ability to identify, protect, defend respond and recover their environment? ☐
4. Are they familiar with the concepts of confidentiality, integrity and availability and how to apply them within their environment? ☐
5. Is there sufficient cross-coverage for each of the roles in compliance with the 80/20 rule? ☐

TOTAL 0

Identity Management

1. Are users created according the correct job roles and is access to folder shares governed by the use of functional groups? ☐
2. Are strong passwords (password complexity) in effect? ☐
3. Do passwords expire on a regular basis? ☐
4. Are all users, especially senior level individuals covered under this policy? ☐
5. Are there limitations on and separation of Administrative and user ID's for elevated access to systems management? ☐

TOTAL 0

Asset Management

1. Are there centrally managed and maintained inventories of computing assetsthat are maintained and audited? (servers, printers, phones, routers, laptops, tablets, etc.) ☐
2. Is there centralized purchase control of computing assets? ☐
3. Are there purchasing and laptop / desktop configuration standards based on job function? ☐
4. Do the configuration standards include encryption, anti-virus, firewalls and only approved software? ☐
5. Are the units configured to automatically apply patches? ☐

TOTAL 0

Risk Assessment

1. Are the staff members able to enumerate the various types of threats to the organization; natural, unintentional and intentional and do they have Incident Response and Disaster Recovery Plans in place? ☐
2. Are the plans practiced, reviewed and updated annually? ☐
3. Is there a documented emergency communications planthat does not rely on a single method, such as group e-mails only? ☐
4. Has the IT and Cybersecurity staff met with steering committee members or various stakeholders to identify both generic and Specific threats to the organization? Example, if the location is near an industrial plant that produces toxic chemicals, is there a plan to deal with Shelter in Place and remote access to data? ☐
5. Has the organization recognized the risk to the safety of individuals, its mission, its assets and its reputation in that order and do the policies and plans put priority on life and safety over all other concerns? ☐

TOTAL 0

Training and Awareness

1. Does the organization have an individual or group tasked with providing cybersecurity training? ☐
2. Does the organization perform cybersecurity as part of onboarding? ☐
3. Does the organization either perform regular annual awareness training or require testing as part of annual HR certification? ☐
4. Does the organization communicate present threats in real-time to the end user community to alert them to be on the lookout for those threats? ☐

TOTAL 0

Access Control

1. Does the organization have an access control plan or policy? ☐
2. Is access control determined by job function? ☐
3. For file server shares and services delivered by a server, is access locked down based on the principle of least access? (only those that require access, receive access) ☐
4. For file server shares and services delivered by a server, is access control by groups only and NOT by any individual user names? ☐
5. Is there some form of physical access control, key and or electronic, between sections of the building, executive wing, wiring closets, server rooms? ☐

TOTAL 0

Data Retention

1. Does the organization have a Data Retention Policy? ☐
2. Does that policy remain in effect throughout the backup and restore process? ☐
3. Is the policy enforced? ☐

TOTAL 0

Data Leakage Protection + PII, PHI, PCI assessment

1. Has the organization identified sensitive data (EX: IP, PII, PHI, PCI) and taken steps to ensure that the data is protected by the principle of least access, is encrypted at rest and in motion where required? ☐
2. Has the organization implemented automated monitoring tools to look for transmittal of sensitive data such as SSNs or based on certain word filtering? ☐
3. Has the organization taken steps to ensure data is protected throughout its lifecycle, even during backup and restore operations and is there a policy or procedure for identifying, communicating and disposing of the data at the end of its useful lifecycle? ☐
4. Has the organization taken steps to educate users that handle sensitive data on the concepts of clear desk and clear screen and have they instituted secure scanning and printing areas or PIN to Print? ☐
5. Does the organization have a plan to identify the extent of the leakage, communicate the impact and provide relief to those affected such as credit monitoring for a specified period of years? ☐

TOTAL 0

Intrusion Detection and Prevention and Network Infrastructure Security

1. Does the organization have a network diagram that accurately conveys the topology of the network architecture with an internally managed IP address scheme? ☐
2. Does the organization or organization's representative configure, maintain, monitor and update their own routers and firewalls? ☐
3. My organization does NOT have any third party or vendor VPN connections into our systems, or if we do, they are isolated, monitored and the third party is contractually obligated to conform to regular cybersecurity assessments. ☐
4. Is WPA2 Enterprise wireless security protocol in use to prevent unauthorized sharing of a WIFI password? ☐
5. Are there any IDS/IPS appliances in place and if yes, do those appliances aggregate and alert with a low frequency of false positives and has the system been tuned to minimize false negatives? ☐

TOTAL 0

Change and Patch Management

1. Does the organization automate the delivery of Critical and High patches to the end user devices? ☐
2. Does the organization regularly apply Critical and High severity patches to the servers? ☐
3. Does the organization test patches before they are released into the production environment? ☐
4. Does the organization have a communication plan for notification of patching and testing of servers? ☐
5. Does the organization log operational changes to the production environment? ☐

TOTAL 0

Backup and Restore and Business Continuity

1. Are backups online, nearline and offline with an air-gap? ☐
2. Have mock recoveries been performed? At the file level? At the server level? ☐
3. Is encryption, data retention and data security maintained throughout the cycle? ☐
4. Is there a Disaster Recovery Plan? ☐
5. Has a mock recovery been performed and if yes, Is continuous improvement part of the after action of mock recovery operations? ☐

TOTAL 0

Physical Security

1. Does the facility require badge access and if yes, is it logged? ☐
2. Is access limited by time of day, day of week? ☐
3. Is human monitoring (guard or receptionist) and/or camera monitoring and a monitored alarm system in place? ☐
4. Does the facility use architectural security principals of lighting, bollards, deterrent landscaping? ☐
5. Do sensitive areas require elevated privileges or dual factor to enter? ☐

TOTAL 0

Incident Response, RCA and CI

1. Is there an incident response plan? ☐
2. Does the plan include real-time communications with staff, outside entities and the media as necessary and appropriate? ☐
3. Is there a help desk or Incident logging application in use? ☐
4. Are Root Cause Analysis part of all after actions? ☐
5. Are issues found and their resolutions part of continuous improvement? ☐

TOTAL 0

Scoring Page

GRAND TOTAL:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	GT
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

How to Calculate your Grade:

Multiply the Grand Total for the 14 sections and multiply x 1.5

Your Score: 0

RESET

SCORE	COMMENTS	
95 and above (Green)	Indicative of mature organization. Training Review, Annual Penetration Testing and Assessments in motion to ensure operational effectiveness are appropriate for this organization.	
90-94 (light Green)	Indicative of an organization that has embraced cybersecurity but is unpolished and may not be able to adapt to emerging and evolving threats. Often, help with the 'finishing touches' is necessary. An Assessment in Motion, training review and Penetration testing are recommended.	
80-89 (Yellow)	Organizations in this range have recognized they are at risk and have adopted many of the fundamentals required to reduce risk and secure data but often have interdepartmental or operational issues that are preventing full adoption, leaving them highly vulnerable to catastrophic systemic failures from major events 'A new set of eyes' to help persuade for the hardest changes is usually necessary.	
70-79 (Amber)	Boilerplate, static defense magazine article best practices are indicated by this score. An organization in this range remains susceptible to and could suffer significant damage from a wide variety of both cyber and business continuity incidents. A Comprehensive Cybersecurity Posture Assessment is recommended.	
60-69 (Red)	An organization in this range would likely be highly susceptible to and may not be able to understand the depth of the damage or be able to recover from an incident that could severely impact continuity of business operations. A Cybersecurity Posture Assessment is highly recommended.	
59 or below (Deep Red)	Indicative of an organization that has not embraced the reality of the threats facing the them or is not engaged in basic cybersecurity practices. Organizations in this range often have a wide range of both identifiable and correctable issues, but lack skills and leadership to help with course correction. A preliminary Cybersecurity Posture Assessment is highly recommended.	

About Decide Consulting

We hope you found this Cyber Security Self-Assessment useful and it provided you team with some valuable thoughts about how to make you company more secure.

decide Consulting is a Houston, TX based IT Staffing and Cyber Security Company. We have been in business since 2004 serving our technology customers.

Business is changing. Technology disrupts. You get to decide what happens.

You need the right people with the right skills at the right time. That's where we come in.