Cybersecurity Preparedness Assessment

for companies of all sizes

Security incidents are unavoidable. Preparations must be in place to quickly identify and respond to an incident. Whether it is a lost laptop or a malicious insider, organizations must be ready to respond. Having a plan available ahead of time is paramount to successfully managing the situation. Although it does take time, there are things that business leaders can do to be prepared, regardless of the size of your company.

Protecting any business should follow a logical, deliberate method beginning with an honest assessment of the organization's current security posture. The assessment should include an inventory of all critical systems, services and processes, as well as business priorities. This assessment will result in the entity's current level of preparedness.

The Greater Houston Cybersecurity Task Force has created the following Preparedness Assessment to assist organizations of all sizes. Complete the survey using the scoring guidance and add up your totals. Compare your totals to the three levels of "Preparedness Scores" on the last page.

Scoring Guidance:

0 : **Don't have or don't perform this activity at all**

1 : **Starting to think about these activities, but no real plan in place yet**

2 : **Try to perform these activities when we can**

3 : **Have documented procedures in place, but could do better**

4 : **Feel comfortable that we are doing the best we can with available resources/budget**

5 : **We got this!!!**

Let's get started!

CYBER HOUSTON

Cyber Hygiene

			Response (0-5)
1		Do you have anti-virus software installed on all your computers and servers?	
2		Do you have a password security standard for users, applications and systems?	
	a	If so, does the standard specify minimum length, complexity, periodic change, maximum password age?	
	b	If so, have you trained your personnel in the use of passphrases instead of passwords and adopted a standard that allows non-complex, long passphrases for authentication?	
3		Are employees and contractors trained on your internal policies and procedures?	
4		Do your employees and contractors sign a non-disclosure or confidentiality agreement stating they will keep information obtained as part of their employment confidential?	
5		Are backups of servers and data performed on a scheduled periodic basis and securely stored off-site (encrypted, locked, and guarded)?	
	a	If so, have you restored data from backups to ensure data is retrievable if needed?	
6		Is there a records management program covering paper and electronic records, including email, in support of applicable regulations, standards and contractual requirements that covers record classification, record retention, and record destruction?	
7		Do you have wireless networks in place using strong encryption (such as 802.11i/WPA2)?	
8		Do you have a data retention and disposal policy and process?	

Risk Assessment

		Response (0-5)
9	Do you have a documented risk management program in place?	
10	Is there a documented risk management procedure, approved by senior management, which defines the process by which risks impacting the confidentiality, integrity and availability of data are identified and managed through resolution?	
11	Have you completed a full risk assessment in the last 12 months that defines each system, threat, risk, impact and mitigation plan to maintain the confidentiality, integrity and availability of data?	
12	Does your organization have the appropriate amount of cyber insurance coverage?	
13	Do you have a comprehensive plan to respond to a breach, including an agreement with a Reputational Risk Advisor?	

Human Resources

		Response (0-5)
14	Do you have a documented employee hiring and termination process in place, including backgrounds checks prior to hiring or allowing access to sensitive information?	
15	Are background checks conducted when employee roles/responsibilities change perpetuating changes in access to sensitive information?	
16	Are security roles and responsibilities of personnel defined and documented in accordance with the organization's information security policy?	
17	Are consequences for non-compliance with company policies written into policies?	

Security Policy / Compliance

			Response (0-5)
18	Do you have a written information security policy that is communicated to all employees?		
19	Do you have a written Information Security Policy that addresses physical access, patching and malware, password use, user administration and roles to limit access, continuous monitoring and encryption of data at rest and in transit		
	a	If so, is the policy communicated to employees, contractors, and service providers?	
	b	Are security policies, procedures, and controls reviewed and tested at least annually?	
20	Do you conduct security and privacy awareness training for employees and contractors?		
	a	If so, is attendance mandatory at least annually?	
21	Do you conduct periodic phishing or other similar attacks to test your employee cybersecurity awareness?		
22	Is there an information security department or individual responsible for security initiatives within the company?		

Physical Security

		Response (0-5)
23	Do you have a plan/procedures in place to evaluate the security of facilities and access to sensitive/controlled areas?	
24	Do you have controls, contracts and or certifications ensuring that access to facilities, sensitive controlled areas and the servers storing your data is secure, protected and limited?	
25	Do you have security procedures for the decommissioning and/or destruction of equipment and storage medium to ensure data can never be retrieved?	
26	Does the organization ensure that critical supporting utilities, such as climate control, fire suppressants and backup power supplies are in place?	

Logical Access

			Response (0-5)
27	Do you have password policy and user authorization procedures and processes in place for granting access to key systems?		
28	Do you have an access control process in place based on least privileged access to systems and confidential information?		
	a	If so, does the process address employment termination and change in status?	
29	Are user access rights reviewed per policy at least annually?		
30	Are privileged/administrator users assigned separate accounts for privileged access to IT and security systems?		
	a	Do you have a password vault/management system for privileged user and system accounts?	
	b	Is your password policy enforced for privileged user and system accounts?	
31	Are user, administrator, and system accounts regularly audited for proper use, rights, time of day and location?		
32	Is Multi-Factor Authentication required for remote access to the network by employees, administrators and third parties?		
33	Is Multi-Factor Authentication required for access to servers, network infrastructure, and critical applications?		

Communications & Operations Management

			Response (0-5)
34		Do you have a patch management program in place to ensure all hardware/software is updated?	
35		Is there an asset management policy or program, approved by management, communicated to appropriate constituents and an owner to maintain and review the policy and to ensure supporting processes are completed?	
36		Do you have a patch management program in place to deploy patches to your environment?	
	a	If so, are critical patches applied within days?	
37		Do you have anti-virus and malware detection systems continuously scanning for vulnerabilities?	
	a	If so, are these systems updated at least on a monthly basis?	
	b	Can non-IT personnel modify or disable these systems on their computers?	
38		Have you deployed firewalls and Intrusion Detection/ Prevention Systems in your environment?	
39		Do you have system configuration and hardening standards for servers, workstations, appliances?	
40		Do you encrypt sensitive data in transit (over public networks, email, etc.) and at rest on servers, desktops, laptops, and storage devices?	
41		Do you have a solid plan in place to store and handle data such as credit cards, Social Security Numbers, or other personally identifiable information that have special requirements?	
	a	If so, do you have the appropriate controls in place to manage this information, including restricting its access to only those with a need to know/need to do?	
42		Do you have a mobile device management policy?	
	a	If so, do you have a mobile device management system?	
43		Do you have a removable media policy?	
	a	If so, is encryption required to secure content in the event of loss or theft?	
44		Is company network access restricted to only approved or company supplied devices?	
45		Are information systems and assets monitored and activity logged to identify cybersecurity events and verify the effectiveness of your security controls?	
46		Do you perform periodic vulnerability scans on your network infrastructure?	
47		Are ongoing external vulnerability scans conducted by a third party?	
48		Do you have a third party perform a penetration test at least annually?	
49		Is there a change management / change control policy or program governing all system, security, and application changes?	
50		Are staging, test and development environments separate from your production environment?	

Information Systems Acquisition / Development

			Response (0-5)
51		Do your software developers think about cybersecurity when developing/deploying solutions?	
52		Is there an automated or other solution to identify authorized software in the organization's environment?	
	a	If so, is there a process in place to identify and remediate unauthorized software?	
53		For software development, do you have a code repository to manage versioning and a back out plan for each change?	

Incident Response

			Response (0-5)
54		Do you have a plan in place for responding to cybersecurity incidents/breaches?	
55		Does the organization have a documented incident response plan covering security, privacy, and business continuity incidents that clearly defines how incidents are identified, classified, mitigated, managed, communicated, resolved and documented?	
56		In the event of a cyber incident or breach, do you have a defined communications protocol for internal and external stakeholders?	
	a	If so, does your protocol include contact information for law enforcement agencies and forensics firms?	
57		Is system audit logging enabled to capture details related to failed and successful authentication attempts as well as any privileged user activity?	
	a	Are audit logs reviewed for potential security events?	
58		Is irregular activity detected in a timely manner and the potential impact of events understood?	

Business Continuity & Disaster Recovery

			Response (0-5)
59		Do you have a documented Disaster Recovery/Business Continuity Plan?	
	a	If so, does the plan include current contact information for key employees and service providers?	
	b	Does the plan identify applications, equipment, facilities, personnel, supplies and vital records necessary for recovery?	
	c	Does the plan include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components?	
	d	Has your Disaster Recovery /Business Continuity Plan been tested in the last 12 months?	
60		Is there an annual management review of the Business Continuity Plan for adequacy of resources (people, technology, facilities, and funding)?	

Vendor Management

		Response (0-5)
61	Do you have processes or procedures to properly vet all your partners/vendors?	
62	Are any aspects of IT services or customer service outsourced?	
63	Is there a documented third-party management program that addresses the security of company and customer data	
a	If so, does the program include security, risk and vulnerability assessment of third parties?	
64	Is there a documented corrective action process to remediate third-party noted issues?	
65	Is there a complete list of affiliated third-parties?	
66	Are third-parties regularly monitored for contractual compliance?	
67	Do your third party contracts include security provisions?	
68	Is there a policy that governs access to the computer systems, data or processing facilities for third parties?	

Let's check your score!

Preparedness Scores (Overall)

0 to 185 : **We have some work to do!**

186 to 325 : **Looking good!**

326 to 460 : **We can all sleep at night!**

	TOTAL
Cyber Hygiene	
Risk Assessment	
Human Resources	
Security Policy / Compliance	
Physical Security	
Logical Access	
Communications & Operations Management	
Information Systems Acquisition / Development	
Incident Response	
Business Continuity & Disaster Recovery	
Vendor Management	
YOUR SCORE