UHY Consulting

The Cyber Savvy CEO

What's your Cybersecurity readiness?

6

Questions to ask your IT Department

As the leader of your organization, the future well-being of the company rests squarely on your shoulders, which includes the security of your network, data and proprietary customer information. Every week in the news, there are reports of companies that have experienced cyber-attacks. While you think it will never happen to you, there's a good chance it could.

Since most likely you're not an Information Technology (IT) expert, we've created this Cyber Readiness Guide with 6 key questions you can use to have a discussion with your IT team about your current cybersecurity readiness.

UHY Consulting

1

Question

Do we have a robust incident response capability in place?

What you want to hear

Yes, we have software that provides alerts and possibly a third-party provider to help monitor our system around the clock and responds through quarantine or other isolation capabilities.

Warning sign

No, we do NOT have anything in place to monitor anomalous or known bad activity on servers, workstations and laptops at all hours.

What can be done immediately

At a minimum, IT should consider deploying a next generation, endpoint detection and response security tools. This type of software is quick to deploy and provides visibility and alerts to help quarantine the infected machine(s) and minimize the extent of the disruption. Better solution options, include active response on your behalf by the trusted monitoring companies.
Determine if IT can respond to the identified issues or they need outside assistance.

UHY Consulting can help you to understand this landscape and navigate these tools.

UHY Consulting

Question

Do we have a regular program to scan our network and applications for vulnerabilities?

2

What you want to hear

Yes, our company has a regular program to scan our network, applications, web services, and networked devices inside and from the internet in place.

Warning sign

No, we do NOT regularly scan our network, software applications and device configurations.

What can be done immediately

Cunning cyber attackers are ready to take advantage of vulnerabilities. Ask IT to conduct a vulnerability scan as soon as they can to begin to identify and patch or remediate any high risk and critical vulnerabilities. At a minimum this should be done quarterly on internal assets and from an internet perspective. For the first few months request the results of the scan.

If they don't have the manpower or resources to support this activity, UHY Consulting can assist.

UHY Consulting


Cunning cyber attackers are ready to take advantage of your company's vulnerabilities.
UHY Consulting

3

Question

Do we have good backups of critical systems, data and configurations?

What you want to hear

Yes, in case of a cyber event, our company has good backups of critical systems, data and configurations and we have tested them. The back-ups are stored offsite or in the cloud so they won't get damaged or deleted.

Warning sign

No, we do NOT have the ability to successfully restore operations from a back-up and/or back-up files are onsite.

What can be done immediately

Work to minimize business continuity risk with your important systems. Confirm that all IT systems are included within the backup solution and ensure that they are tested periodically to work when needed. Treat backup files as critical data and ensure the backups are segmented and isolated from the rest of the network. Also, ensure a full copy of the backups is stored offsite and is inaccessible to any ransomware or malware that might break loose in your environment.

UHY Consulting can provide additional advice, testing or design ideas for your overall backup strategy.

UHY Consulting

Question

Do we have an incident response plan for a cyber-attack?

Warning Sign

No, there is NO cyber-attack or overall incident response plan.

4

What you want to hear

Yes, our company has a solid plan in place that has been regularly tested and our employees understand their roles and actions depending on the situation.

What can be done immediately

You can't wait for a cyber-attack to occur to build an incident response plan. At a minimum, identify who your employees need to contact if a cyber incident is happening. Document the expected actions to be performed in the event of an incident and perform some tabletop tests of the plan before a real event occurs. You may want to consider a cyber 911 call service that will quickly focus the incident response activities to stabilize the environment and begin the recovery process.

UHY Consulting offers a full incident response team specializing in preventative and reactive measures for incidents and/or breaches.

UHY Consulting


Don’t put your
company’s brand,
your clients’ trust
and your future
at risk.
UHY Consulting

5 Question

Do we have an employee security awareness program?

What you want to hear

Yes, our employees are our best source of defense and we have a continuous testing program in place, so our staff stays alert and vigilant.

Warning Sign

No, our employees do NOT understand the extreme threat that phishing emails can pose to our company.

What can be done immediately

Phishing emails remain the easiest and most likely way to get into your business to steal data, access your internal network or begin the staging of malicious software. IT or an outside vendor can build an internal program to train and educate them about suspicious emails in their inboxes, instant messages, texts and calls.

UHY Consulting, can provide phishing testing and social engineering training as well as track your employee's progression.

UHY Consulting

Question 6 Do we have cyber insurance?

What you want to hear

Yes, we have a cyber insurance policy that clearly outlines what the policy does and does not cover and we understand the carrier's role versus your role. For operational risks not covered by insurance, our company has taken the proper steps.

Warning Sign

No, we do NOT have a cyber-attack or overall incident response plan.

What can be done immediately

Don't put your company's brand, your clients' trust and your future are at risk. An insurance broker can provide guidance on a policy and help you manage your risk appetite for a cyber loss. Ask specific questions on what losses are covered, including such things as public relations, ransomware payments, incident responders and digital forensics.

UHY Consulting can provide industry contacts and expertise to assist in selecting the right cyber insurance provider and recommended coverage types.

UHY Consulting

6

Don't let cyber criminals negatively impact and, possibly destroy, your company. It's critically important to develop a plan to mitigate the risk of a devastating cyber-attack. Our Cybersecurity experts address cybersecurity as an enterprise business risk.

The cornerstone of our methodology is to translate IT risks into business risks and provide meaningful insight to our stakeholders – from the boardroom to the security engineer. Let's talk about your cybersecurity posture and the best roadmap for your company.

Questions to ask your IT Department

We take a facilitated approach to determine the optimal assessment type and tailor each cybersecurity engagement to the individual needs of our clients.

UHY Consulting

Let's connect!

Norman Comstock | 713-325-8680 | ncomstock@uhy-us.com
Richard Peters | 713-325-8684 | rpeters@uhy-us.com
Kimm Anderson | 314-615-1275 | kanderson@uhy-us.com

UHY Consulting