nxtconcepts

Crisis Website Audit Checklist

During an emergency knowledge is power. Managers and employees must be able to communicate effectively, both internally to staff and externally to the public. To help alleviate business disruptions, use this checklist as a starting point to develop a website strategy and define processes and protocols.

Website domain (URL)	
	Where is the domain registered?
	What is the expiration date for the domain?
	Who is the Domain Admin contact at the registrar?
	Who is the Domain Technology contact at the registrar?
	What is the registrar login URL?
	What is the username and password to login to the registrar?
	Verify the SSL Certificate. When is the expiration date?
Website Hosting	
	Who is your hosting company?
	What kind of server do you have? Shared, VPS or dedicated?
	What kind of hosting plan are you on? How much bandwidth are you using? Is it expandable in case of spikes in usage?
	How do you contact support? Phone number, email, live chat?
	Who has access to the server? IT Manager? 3rd party vendor?
	Does the hosting company have a business continuity plan to keep servers up and running?
	What is the average uptime (server reliability)?
	Do you have a monitoring service to track server performance?
Business Emails	
	Where are your company emails hosted?
	Who creates or manages email accounts?
	Who do you contact if your email stops working?
	Do you have a backup email to use if company emails are not available?
	When was the last time it was required to update passwords?
	Do all devices accessing company email have virus and malware protection?
	Take inventory. Are there any non-used emails that should be removed from the server for security and to save space?
	How many email forwards are in place? Do any need to be removed?

Website Software	
	What kind of CMS or platform is your site built on?
	Who has access to login and make changes?
	Are CMS security patches and updates current?
	If you have installed extensions/plugins how old are they and do they have the latest updates?
	Do you have automatics daily backups running?
	Are your backups offsite or off the server where the website is hosted?
	What is your backup recovery plan?
	When was the last time a backup was restored, and the integrity tested to make sure they are not corrupted or otherwise unusable?
	Are there any third-party integrations that could cause an issue if they are disrupted? I.e. weather apps, webcams, social feeds.
	What emergency support options do you have for the site software if there is an issue?
	Do you have a firewall on your server? If so, who is the vendor?
	Are there regular malware scans running on the website files?
	Do you regularly check that your site is not blacklisted at blacklist authorities such as Google or McAffe SiteAdvisor?
Employees	
	Is their home wifi password protected?
	Have they changed their email or website login passwords in the last 30 days?
	Is there an automatic virus scan on their devices?
	Have managers reinforced that employees should be hyper aware of not clicking on links from unknown email senders nor download software from unknown websites?
	Are employees backing up company work each day?
	If employees have a problem with the website or email, who do they contact? Are their enough resources with large numbers of remote workers needing support?
	Have employees that need access to the website provided their IP address to be added to the website firewall so they are not blocked from access?
	Do you and your employees have a list of all the website related suppliers? Have you contacted them to be alerted to any issues they may be having?
	If employees connect using a VPN, how much capacity can your VPN handle?

Resources for Additional Reading

US Government Recommendations for an IT Recovery Plan https://www.ready.gov/business/implementation/IT

Cyberthreat Real Time Map https://cybermap.kaspersky.com/