

A cyber attack, like ransomware, can infect an entire network within minutes once it gains access to a system. Files will be locked or encrypted, while cyber-criminals demand payment for access to your data. If paid, these criminals may or may not provide the necessary fix. Worse yet, paying ransom encourages this malicious activity and may even make you a target for future cybercrime.

Take these measures now to secure vulnerabilities, and prevent a cyber attack.

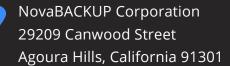
V-	inventory management
	Catalog all the software which is deployed throug There are no unsupported operating systems (Wi No unauthorized software (non-business file shar There are no unknown/unmanaged computers, a
	No unauthorized software (non-business file sh
8)	Patch Management
	All servers have managed Windows patches and a
	All workstations have managed Windows patches
	All other operating systems have regular patch m
	All applications and their patches are maintained
	Monitoring is in place

	Firewall
	Running a business grade firewall, not a consumer firewall Advanced filtering, intrusion detection, layer 7 traffic classification, and firewall is fully managed Running latest version of firewall software and managed updates Monitoring firewall alerts
Ê	Antivirus Software
	Running a business grade AV, not a consumer AV All servers and workstations are running AV that is real-time scanning Centrally managed and updated Policies setup in AV to block execution of harmful executables, along with alerting Monitoring AV alerts
	Backups
	All machines that have critical data on them are backed up Images of servers are done at least monthly File backups are run daily Following 3-2-1 backup rule (3 backups, stored on 2 different media, with 1 offsite) Testing restores from backups at least monthly Monitoring backup failure reports
	Filtering
	Antispam/anti-phishing in place Filtering file attachments in email (.exe, scr, .com, etc.) DNS filtering in place Show file name extensions in Windows

(55)	Web Browsing		
	Disable all unnecessary scripts/plug-ins Browsers are up-to-date and running latest versions of required plug-ins		
	Permissions		
	Enforce principle of "least privilege" on systems and data Software restriction policies put in place to prevent programs from executing from common ransomware locations (temp folders, etc.)		
Op.	Advanced Prevention		
	Group policies Periodic port/vulnerability scans Inspect network periodically to disable any unnecessary/vulnerable services Segment network for servers, backup, data, end-points Disable bootable devices like CD/ DVD and unnecessary USB ports for flash drives, etc. Enable BIOS Password Authentication		
	Training		
	Security awareness training: Offer examples of what to avoid Simulated attacks (phishing, etc.) with action plan (ex: Disconnect from network / Wi-Fi)		
<u>O</u>	Cyber Insurance		
	Consider adding cyber-liability insurance to protect your organization from the financial costs associated with a cyberattack, ransomware attack or other online hacking threat.		
About NovaBACKUP Corporation			
	NovaBACKUP Corporation specializes in local and cloud-based backup and disaster recovery for managed service providers and professional offices. With over a million machines protected and		

over twenty years in the market, NovaBACKUP's goal is to deliver high-performance, reliable and affordable data protection worldwide.







Tel.: (805) 579-6700 Fax: (805) 579-6710 Email: ols@novabackup.com www.novabackup.com