Barkrum

RESOURCE · QUICK CHECKLIST

Ransomware Readiness Quick Checklist

A fast self check against the essentials that stop most ransomware, and speed recovery from the rest.

This checklist is organized around the six functions of the NIST Cybersecurity Framework 2.0, following the structure of the NIST Ransomware Risk Management Profile (NIST IR 8374r1). **It is a starting point, not a substitute for a full assessment.** Each item you cannot check is a place worth a closer look.

> **How ransomware usually gets in:** *phishing, exposed remote access, and unpatched systems. Most successful attacks exploit basics that were left undone. The items below are ordered the way NIST orders them, from governing the risk through recovering from an event.*

GOVERN · Set the direction and accountability

- ☐ **Ownership assigned.** Someone is clearly responsible for cybersecurity and for the ransomware response plan, even if that role is outsourced.
- ☐ **Risk understood.** You know what a ransomware event would cost your organization in downtime, data, and reputation, and you plan accordingly.
- ☐ **Vendors accounted for.** The third parties who touch your systems and data are known, and their security is part of your own risk picture.
- ☐ **Cyber insurance reviewed.** You know what your policy requires of you, since coverage increasingly depends on controls like multifactor authentication and tested backups.

IDENTIFY · Know what you are protecting

- ☐ **Asset inventory maintained.** You have a current list of the devices, systems, and software that run your organization, so nothing critical is invisible.
- ☐ **Data located and prioritized.** You know where your most important and sensitive data lives, and which systems you could not operate without.
- ☐ **Vulnerabilities tracked.** You regularly identify weaknesses in your systems, including exposed remote access and out of date software.

PROTECT · Put the safeguards in place

- ☐ **Multifactor authentication enabled.** MFA is turned on for email, remote access, and any system reachable from the internet. This single control stops a large share of attacks.
- ☐ **Software kept patched.** Operating systems and applications are updated promptly, closing the vulnerabilities ransomware most often exploits.
- ☐ **Least privilege enforced.** Users and accounts have only the access they need, and administrator rights are tightly limited and separated from daily use.
- ☐ **Endpoint protection deployed.** Modern anti malware or endpoint detection is running on every device that can reach your network.
- ☐ **Email and web filtering active.** Phishing and malicious links, the most common entry point, are filtered before they reach staff.
- ☐ **Remote access secured.** Remote desktop and VPN access is closed to the open internet, protected by MFA, and monitored.

- ☐ **Staff trained.** Your people can recognize a phishing attempt and know how to report one, because they are the first line of defense.
- ☐ **Backups protected.** Backups exist for all critical data and are kept offline or immutable, so ransomware cannot encrypt or delete them along with the originals.

DETECT · Catch it early

- ☐ **Monitoring in place.** System and network activity is logged and watched for the unusual behavior that precedes or accompanies an attack.
- ☐ **Alerts reach someone.** Security warnings actually reach a person who will act on them, rather than filling an unread inbox.
- ☐ **Logs retained.** Activity logs are kept long enough to investigate an incident and understand how it happened.

RESPOND · Have a plan before you need it

- ☐ **Incident response plan written.** A documented plan exists for a ransomware event, covering who to call, what to isolate, and how to communicate.
- ☐ **Roles and contacts defined.** Everyone knows their role, and the contact list includes leadership, IT, legal, insurance, and law enforcement.
- ☐ **Containment steps ready.** You know how to quickly isolate affected systems to stop ransomware from spreading.
- ☐ **Plan practiced.** The response plan has been walked through in a tabletop exercise, so the first time is not during a real attack.

RECOVER · Get back to operating

- ☐ **Recovery plan documented.** A written plan describes how to restore systems and data, and in what order, after an event.
- ☐ **Restores actually tested.** You have restored from backup and confirmed it works, rather than assuming the backups are good.
- ☐ **Recovery time understood.** You know roughly how long it would take to get critical systems running again, and whether that is acceptable.
- ☐ **Lessons captured.** After any incident or test, what you learned feeds back into the plan so readiness improves over time.

Not sure where you stand?

A Barkrum Ransomware Readiness Assessment turns this checklist into a measured, documented picture of your posture against the NIST framework, with a clear plan to close the gaps. The same report also gives you the evidence cyber insurers increasingly ask to see.

www.Barkrum.com

Educational resource based on the NIST Ransomware Risk Management Profile (NIST IR 8374 Revision 1) and the NIST Cybersecurity Framework 2.0. General guidance, not a guarantee of protection or a substitute for a full assessment.