RLS CYBERSECURITY

CYBER INCIDENT READINESS CHECKLIST

A practical starting point for reducing cyber risk and improving your response

Cyber incidents become far more damaging when organizations are unprepared to detect, contain, and respond quickly. While no business can eliminate every risk, organizations that understand their risks, implement core protections, and prepare for incidents in advance are often able to reduce operational, financial, legal, and reputational impact significantly.

Use this checklist as a starting point to help evaluate your organization's readiness. It is by no means a complete checklist and is intended to be a starting point. Consult a professional for further guidance.

Understand Your Risks

- ☐ Identify the systems, accounts, and data that would create the greatest impact if compromised
- ☐ Understand where sensitive information exists and who has access to it
- ☐ Evaluate third-party vendors and trusted partners that could introduce risk into your environment
- ☐ Consider the likelihood and business impact of common threats like phishing, credential compromise, wire fraud, ransomware, and business email compromise
- ☐ Determine whether your organization should complete a formal cybersecurity risk assessment based on your industry, size, regulatory obligations, or data exposure

Strengthen Core Security Practices

- ☐ Use Multi-Factor Authentication (MFA) for critical accounts and remote access
- ☐ Review email security and user protections against phishing and malicious attachments
- ☐ Properly set email security configurations for SPF, DKIM, and DMARC
- ☐ Provide ongoing security awareness training and encourage users to report suspicious activity immediately
- ☐ Implement Endpoint Detection & Response (EDR), logging, vulnerability management, and monitoring tools
- ☐ Understand how privileged accounts, stored passwords, and remote access are secured
- ☐ Ensure cybersecurity responsibilities are clearly owned internally or through trusted third-party providers

Prepare for a Cyber Incident

- ☐ Develop and maintain an Incident Response Plan tailored to your organization
- ☐ Identify your Incident Response Team, including internal leadership, IT, cybersecurity, legal, insurance, and external partners
- ☐ Establish offline communication methods in case email or business systems become unavailable
- ☐ Define what events or conditions should trigger your Incident Response Plan
- ☐ Understand how incidents will be documented, escalated, investigated, and contained
- ☐ Review cyber liability coverage and understand reporting requirements, response resources, and policy limitations

Improve Detection & Containment

- ☐ Train staff to report unusual or suspicious activity quickly, even if they are unsure
- ☐ Review cybersecurity alerts and suspicious activity with urgency
- ☐ Be prepared to isolate compromised systems and revoke sessions quickly
- ☐ Preserve logs and evidence for investigation before wiping or restoring systems
- ☐ Understand breach notification obligations, contractual requirements, and reporting timelines in advance
- ☐ Conduct tabletop exercises or incident response drills to test your plan before a real incident occurs

SUCCESSFUL INCIDENT RESPONSE

No one can guarantee that nothing bad will ever happen. The goal with cybersecurity is to reduce the likelihood of incidents, detect issues quickly, contain damage effectively, and recover with as little disruption as possible.

Organizations that prepare in advance are often able to respond faster, reduce losses, and avoid the confusion and delays that make incidents significantly worse.

Need Help Getting Started?

A checklist alone is not enough to fully prepare an organization for today's cybersecurity risks. Building an effective cybersecurity and incident response strategy often requires guidance, coordination, technical expertise, and ongoing improvement.

Work with experienced cybersecurity and risk professionals to:

- better understand your risks
- evaluate your current readiness
- improve your security practices
- build and test an incident response plan
- align cybersecurity efforts with your business and operational goals

Join us for a free Cyber Strategy Session to get more actionable advice and additional resources:

rlsconsulting.co/freecyberconsult
info@rlsconsulting.co

RLS CYBERSECURITY