10 WAYS TO IDENTIFY
CYBERSECURITY GAPS

The complexity of our systems and networks makes ongoing monitoring for security gaps critical. Find and close vulnerabilities with these strategies.

ASSESS YOUR RISKS

Identify all possible sources of risk (e.g. cyberattack or natural disaster) and rank their likelihood. This sets you up to establish strategies to effectively take action.

EDUCATE EMPLOYEES

Humans are, regrettably, the weakest link. Ensure your people are security aware and participate in ongoing training to contribute to your cyber defense.

PERFORM
VULNERABILITY SCANS

Running regular scans to identify potential weaknesses and flaws can protect you against breaches and sensitive data exposure.

MONITOR
INFRASTRUCTURE

Set up a system to track network traffic, processes, and services to ensure correct functioning and proactively identify external threats.

AUDIT CYBERSECURITY
PRACTICES & POLICIES

Periodically evaluate whether you're following industry standards for information security management.

EVALUATE PHYSICAL
SECURITY

Periodically evaluate whether you're following industry standards for information security management.

CREATE AND TEST A
DISASTER RECOVERY PLAN

Planning for the worst will help you identify what can occur and determine what gaps could arise from an incident.

CONSIDER THIRD PARTY
OR VENDOR RISK

Reviewing and assessing your external partners' security levels can help ensure attackers can't exploit those connections to access your network.

HAVE EXPERTS PERFORM
PENETRATION PEN TESTING

In pen testing, a cybersecurity expert views your setup through the eyes of a hacker to identify areas of improvement.

PARTNER WITH A MANAGED
SERVICES PROVIDER (MSP)

A security partner can provide 24/7/365 network monitoring, perform security audits, and help train your people in cybersecurity best practices.

The systems you use maintain are inevitably vulnerable. Cut your risks today, by contacting DP Computing today.

www.dpcomputing.com.au

DP COMPUTING