Ensure Cyber Security Readiness with a Midsummer Fitness Checkup

With hot, sunny days at the beach or on the trail, summer brings a renewed dedication to getting fit. Just like a tired worker who has spent too many long days behind a desk, organizations need a fitness check, as well. Invest time this summer into assessing cyber security readiness. Use the following tips to start the process off right.

Double-check Essentials of Basic Cyber Security Readiness

Every fitness checkup starts with the basics. For instance:

- Update patch management processes – Keep software, firmware, and operating systems up to date by applying patches promptly. Set up automatic updates where possible
- Review backup plan and test data backups – Set up regular, automated backups. Keep in mind remote workers, as well as data both on premises and in the cloud. Keep three copies of data, including a copy stored offsite. Encrypt all backups and test the backups regularly.
- Enforce strong password policies – Hackers love a weak password, as it provides them an open door into your system. Implement password policies that enforce strong passwords, require regular password change, and prevent users from reusing their previous passwords. Better yet, utilize multi-factor authentication.

- Improve security awareness training – Take steps to improve employee training to be more targeted and engaging. In particular, phishing awareness training can prove critical in guarding against the most common threats.

Conduct Risk Assessments

With the basics underway, take a deeper dive by engaging a security consultant to run a security evaluation. The consultant will look at the organization from the viewpoint of a hacker to uncover existing vulnerabilities. This includes identifying information technology assets, as well as reviewing existing security policies and controls.

Use the results of the risk assessment to prioritize security efforts moving forward. Then, to take risk assessment even a step further, consider running penetration testing. This involves white hat hacking attempts to test for vulnerabilities in a realistic situation.

Review Access Management

Summertime cyber security fitness checking offers the perfect time to review access controls and make necessary adjustments. For instance, be sure that persons no longer employed by the organization no longer have access to the system.

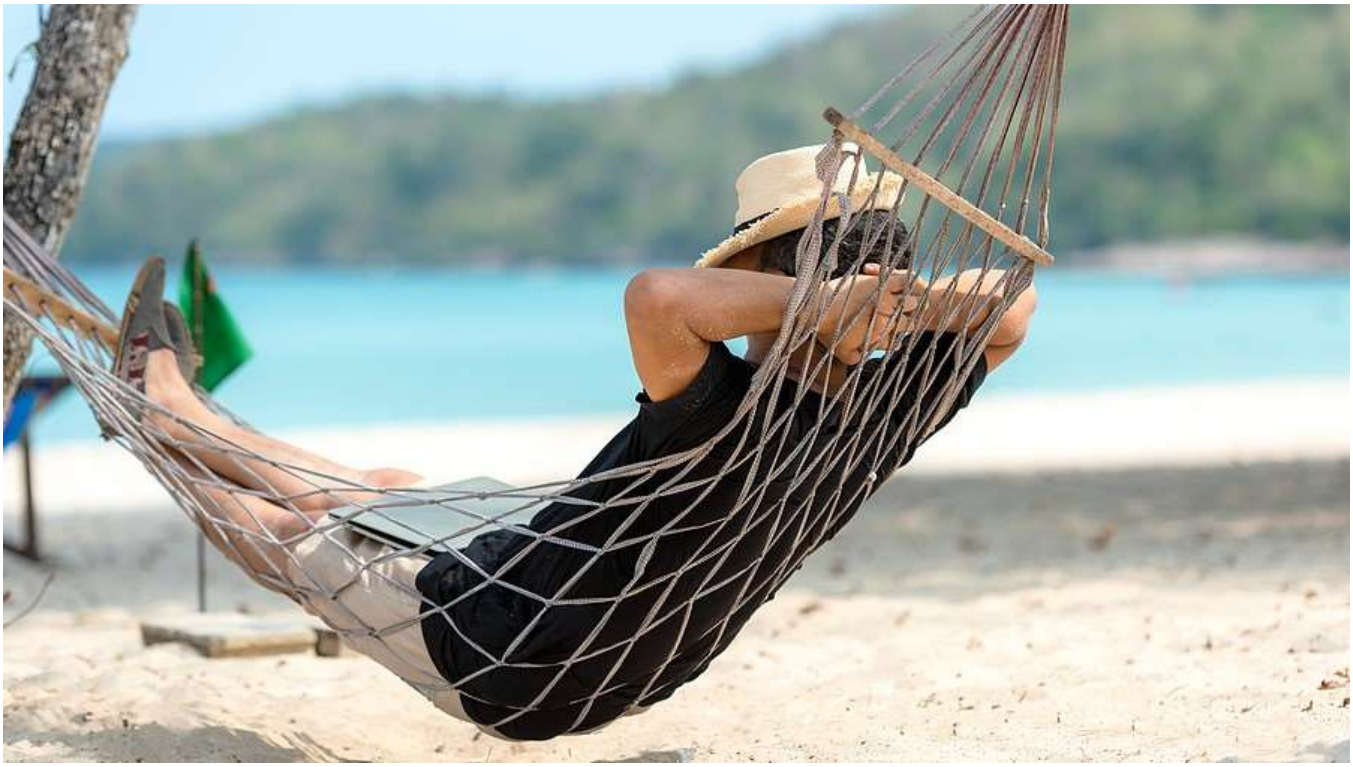
Additionally, implement role-based access and restrict access for all employees to only those areas and functions that they need to perform their jobs. In particular, narrowly limit the number of persons with administrative access to IT infrastructure.

Test Disaster Recovery Plan

Every organization needs a disaster recovery plan if a natural disaster, technical failure or cyber-attack impacts digital assets. This should include key personnel and their roles, a communication plan, and steps to take at every stage of the incident.

Think of specific information that could prove critical. For example, recovery personnel will need to know administrative passwords and understand which applications and resources have priority. They also need to know who to alert and when to involve law enforcement personnel.

Any significant changes to personnel, insurance coverage, regulations or the IT environment will necessitate updates to the recovery plan. Additionally, organizations should test disaster recovery plans at least annually to work out bugs and ensure a quick recovery process.



Enlist Expert Help

The security experts at eMazzanti offer free cyber security assessments to get you started. In a time of security personnel shortages, we stay updated on the latest tools and trends in cyber security. We also keep on top of emerging cyber threats and changes in the regulatory environment.

eMazzanti consultants help organizations move past checkbox compliance to implement comprehensive cyber security strategies tailored to business needs. From initial risk assessment to network security, email defense and continuous monitoring, eMazzanti has the options you need to balance productivity and security.