VALOR
CYBERSECURITY

EXECUTIVE SUMMARY

In conducting a comprehensive cybersecurity assessment for your business, Valor Cybersecurity utilized our proven Top 10 Best Practice Checklist. This thorough examination encompassed key areas crucial to digital security. Our experts meticulously evaluated your organization's current cybersecurity posture and identified vulnerabilities. The resulting executive summary provides a condensed overview of our findings, highlighting the top 5 prioritized recommendations for fortifying your digital defenses. This report aims to empower your business with actionable insights, ensuring robust data protection and compliance.

1

We noticed one of the constraints/vulnerabilities we discovered in your company (Golf Galaxy) was Annual Digital Risk Checkup. We noted there was a lack of a formal inventory.

Recommendation: consider online applications (e.g., Google Drive) to formalize the inventory for virtual/physical assets. A physical document can be timely to implement, so having an online document can speed up the inventory process.

FIRST

2

After the formalization of the inventory, create and maintain copies of the inventory before applying changes, such as when adding new physical assets (e.g., computers). This action is essential for discovering specific vulnerabilities of your assets. Several copies of the inventory offer backups, but it also provides a history of what has been added and removed.

THEN

3

One of the other constraints was Backup Data and Software, then Test. We noted there were weak backup standards/operations.

Recommendation: consider using the 3-2-1 rule for backups. This means three copies of the original data, two different medias (e.g., Hard drive and cloud storage), and one copy located offsite.

NEXT

4

One of the other constraints was Employee Bootcamp. We noted there was a lack of cybersecurity awareness within your workplace.

Recommendation: consider using a free employee cybersecurity awareness training program, such as those offered by the Cybersecurity Infrastructure Agency (CISA). Awareness can prevent social engineering attacks that target your employees.

AFTER THAT

5

Alternatively, or in conjunction to, consider discussing cybersecurity topics/events (e.g., the 2021 Colonial Pipeline Attack) within the workplace. It can be hosted as a short formal meeting or as small talk. Additionally, consider introducing prevalent topics such as phishing, malware (malicious software), and social engineering in general.

FINANLLY

VALOR
CYBERSECURITY

400 Granby Ave, Norfolk, Virginia 23510, USA
Contact us at info@valor-cybersecurity.com

Schedule Your Next Steps

Partner with us, we are ready to help.