XYZ LIMITED

Risk Assessment Board Summary

Abstract

Our assessment summary provides an overview of the current security posture of the organization. The report is a combination of a risk analysis done by our V-CISO through security assessment, Security Ratings by Security ScoreCard, and Phishing Simulations.

Itellisecure Pvt Ltd

14/04/2021

Executive Summary

The Risk Assessment provides a high level overview of the risks arising from the internal and external threats exploiting the weaknesses in the People, Process and Technology Pillars of Cyber Security Function, thereby enabling your organization to further strengthen your Cyber Security in 360Degree with Defense in Depth and Breadth Approach.

Cyber Security Control Security Score Card

Based on the assessment done by our Cyber Security Experts on your responses provided to the Questionnaire, refer the figure 1 for Cyber Security Control Score Card which provides individual Cyber Security Control Domain Wise – Maturity Level Vs Risk Rating

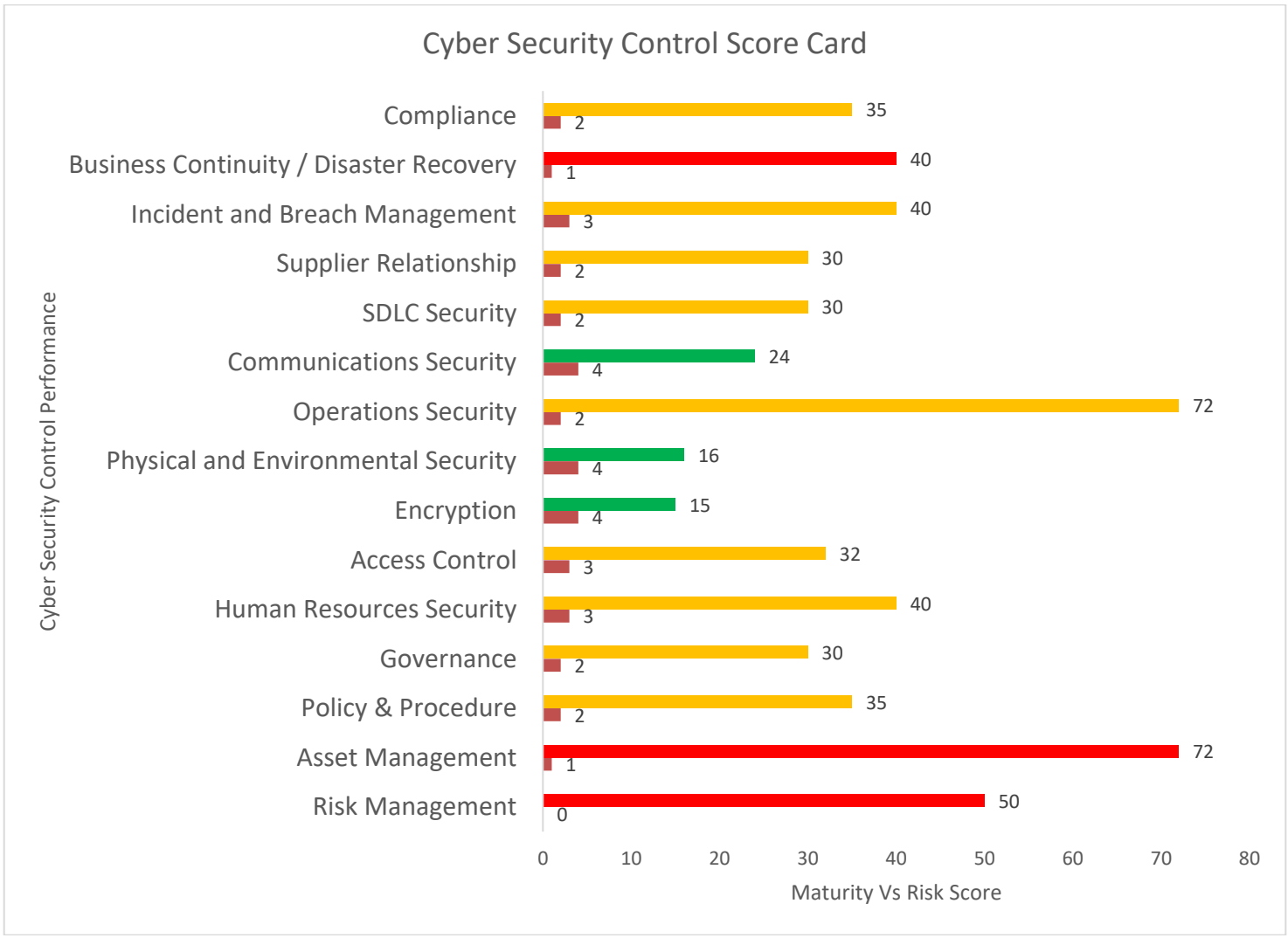


Figure 1

Overall, the Cyber Security Control Score Card provide MEDIUM Risk to your organization from the IT Landscape.

Figure 2, provides Maturity vs Risk Score Card for the IT General Controls of your organizations. IT General Controls are common minimum cyber security controls which any organization must focus first to achieve some quick gains on their Cyber Security Program.

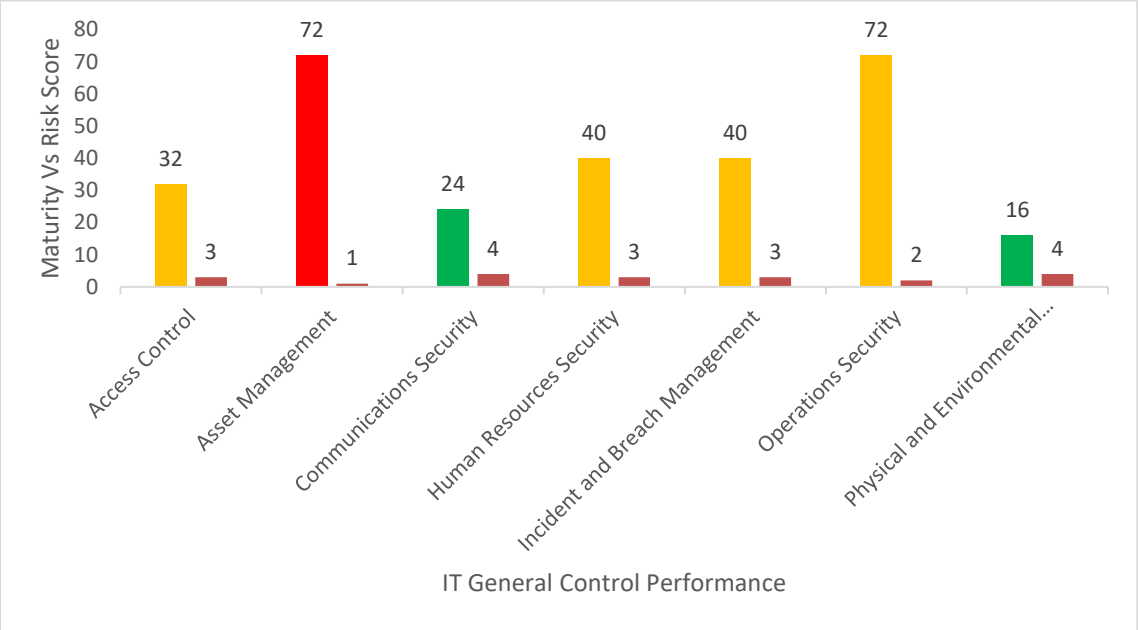


Figure 2

Figure 2, provides Maturity vs Risk Score Card for the IT General Controls of your organizations. IT Specific Controls are those special controls which any organization must focus to further streamline and gain value from their Cyber Security Program.

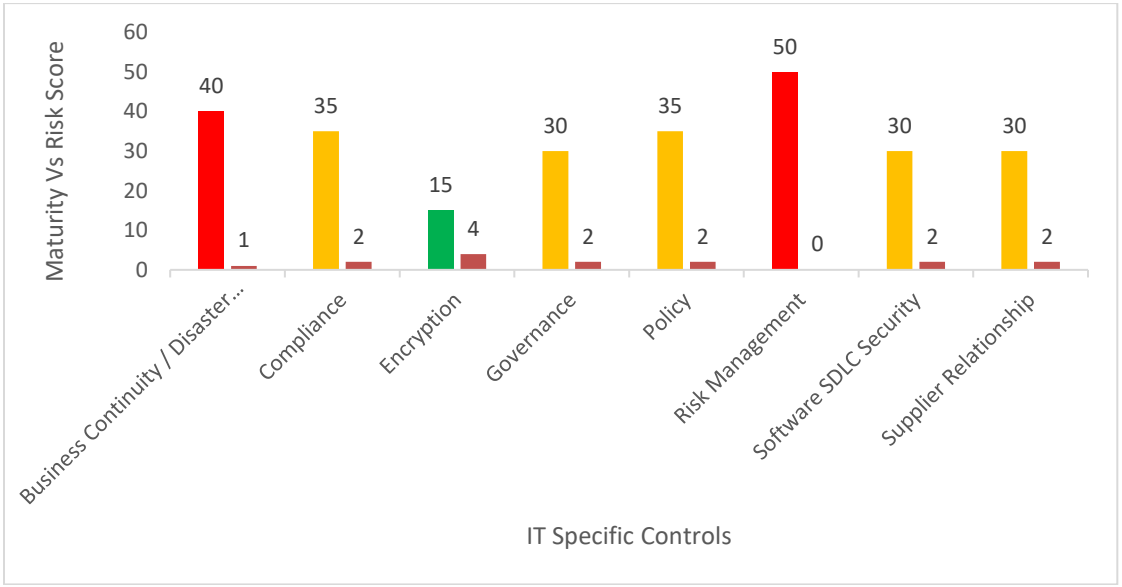


Figure 3

SECURITY SUMMARY REPORT

Scorecard for
XYZ Limited

Generated October 28, 2020
by _____@securityscorecard.io), SecurityScorecard

SecurityScorecard

C 74

Threat Indicators

D 66
NETWORK SECURITY
Detecting insecure network settings

A 90
DNS HEALTH
Detecting DNS insecure configurations and vulnerabilities

C 75
PATCHING CADENCE
Out of date company assets which may contain vulnerabilities or risks

F 46
ENDPOINT SECURITY
Measuring security level of employee workstations

A 100
IP REPUTATION
Detecting suspicious activity, such as malware or spam, within your company network

B 81
APPLICATION SECURITY
Detecting common website application vulnerabilities

A 100
CUBIT SCORE
Proprietary algorithms checking for implementation of common security best practices

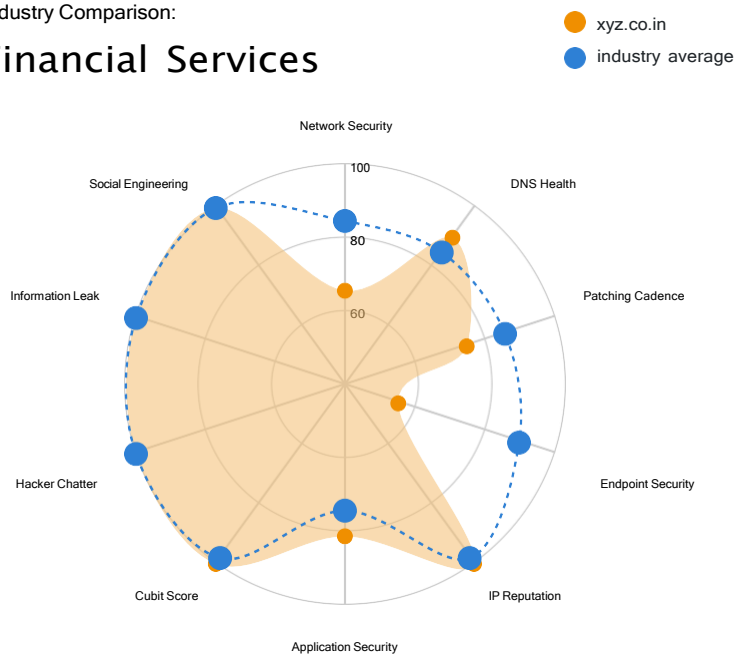
A 100
HACKER CHATTER
Monitoring hacker sites for chatter about your company

A 100
INFORMATION LEAK
Potentially confidential company information which may have been inadvertently leaked

A 100
SOCIAL ENGINEERING
Measuring company awareness to a social engineering or phishing attack

Industry Comparison:

Financial Services



VULNERABILITIES	MEASURE
Open Ports	7
Site Vulnerabilities	16
Malware Discovered	5
Leaked Information	0

Phishing Simulation Report

A follow-up Phishing Simulation was conducted on XYZ domain on 1st November 2020. A change password email was sent out to track user behavior. Once the users clicked on the embedded link in the email, they were redirected to a webpage that provided them on-the-fly training. This training provides the opportunity to educate the users and decrease the phish % over time.

Campaign Results

The emails went out to 500 users, out of which 400 users opened the email and 80 users clicked on the phish link embedded in the email.

Emails sent	Emails Delivered	Emails Opened	Failures/ Clickers	Phish Prone %
500	500	400	80	16 %

Phish % Comparison

Phish Percentage is calculated from the total number of phishing test failures divided by the number of emails delivered.