Security Summary Report

Report generated 3/15/20 by **Security**Scorecard

We are sharing this independently-gathered confidential business insight that may help inform your policy decision.

C 74 | New York University
nyu.edu

Threat Indicators

D 65 **NETWORK SECURITY**
Detecting insecure network settings

D 69 **DNS HEALTH**
Detecting DNS insecure configurations and vulnerabilities

C 70 **PATCHING CADENCE**
Out of date company assets which may contain vulnerabilities or risks

C 72 **ENDPOINT SECURITY**
Measuring security level of employee workstations

C 77 **IP REPUTATION**
Detecting suspicious activity, such as malware or spam, within your company network

C 72 **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
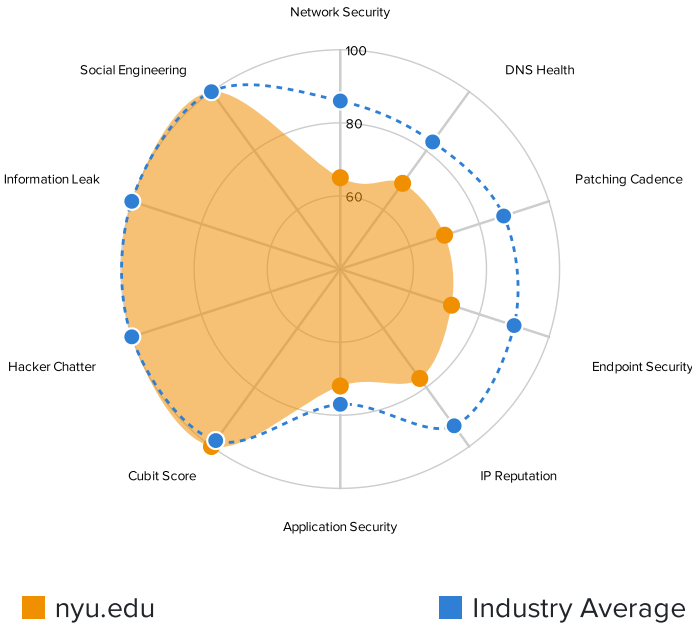
A 100 **INFORMATION LEAK**
Potentially confidential company information which may have been inadvertently leaked

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

Industry Comparison: Education

■ nyu.edu   ■ Industry Average

Vulnerabilities

VULNERABILITY TYPE	MEASURE
Open Ports	371
Site Vulnerabilities	177
Malware Discovered	53
Leaked Information	0

SecurityScorecard