CyberRisk Alliance
CYBERSECURITY COLLABORATIVE

Planning for 2020 Cyber Attacks: Are You Ready?

Threats to attack, infiltrate, and exploit computer systems, networks, and data-dependent organizations (and their brand, reputation, and financial wellbeing) are on the rise. Forecasts are often consistent year-over-year: this year will be worse than last year.

Regardless of industry, customer segment, or organization type, the question to answer for this year is a ubiquitous one: are you ready?

Can you, your cyber defense systems, and your workforce outwit the malicious savviness of attackers and the destructive consequences of compromised data ruining your business?

This artifact serves as an assessment or audit of your defense readiness against common types of cybersecurity attacks. The following is a general rating scale of your (self-assessed) organizational cyber-attack security maturity. For each attack type, rate your security maturity relative to people, process, and technology in place to defend against attacks by noting a number to represent Low (1), Medium (2), or High (3) level of preparedness.

[Note: 1 in the left columns of General Preparedness, 2 in the center columns of General Preparedness, or 3 in the right columns of General Preparedness). Use the righthand column to detail immediate action items and next steps based on your organizational security readiness for the attacks this year.

	LOW (1)			MEDIUM (2)			HIGH (3)		
	People	**Process**	**Technology**	**People**	**Process**	**Technology**	**People**	**Process**	**Technology**
General Preparedness	No dedicated function to test or monitor	Ad-hoc or low-level defense standards to test, monitor, recover	Little to no defense-in-depth software or hardware systems	Established functions with some dedicated staff who test and monitor	Some process standards in place but not fully in place across the firm	Some defense-in-depth software or hardware systems covering some assets for some/part of attacks	Fully dedicated staff and functional coverage to fully test and monitor	Process standards are in place across the firm and are regularly and fully tested against target levels and goals	Extensive defense-in-depth software or hardware systems covering all critical assets for full array of attacks

	General Preparedness									
	LOW (1)			MED (2)			HIGH (3)			
Common Cyber Attack Type	**P**	**P**	**T**	**P**	**P**	**T**	**P**	**P**	**T**	**Action Items**
Phishing: used to steal personal user data by posing as a trusted source; tricking victims into opening a text message, email, or clicking on a link that freezes a system, reveals critical information, or installs malicious code. [note: there are specific types of *phishing* such as spear, which is aimed at a specific individual or organization and *whale*, which is aimed at high profile people such as a CEO.]										
Malware: stealthy code aimed to affect systems without user consent and that can spread from user to user and network to network. [note: examples of malware include ransomware, drive-by attacks, and trojan horse schemes.]										
Web: these attacks are focused on backend database information and carried out often by SQL Injection or cross-site scripting with the intent of accessing customer lists, personal details, and company data.										
Authentication: attempt to hack, decrypt, or simply steal a user's password with criminal intent and is often carried out with password sniffers, dictionary attacks, and other cracking algorithms and software programs.										
Eavesdropping: also known as snooping or sniffing, this is a network attack that attempts to steal data being sent/received via smartphone or other digital device. [note: another type of eavesdropping in Man-in-the-Middle (MITM) attacks.]										
Birthday: a statistical phenomenon and a simplified version of a brute-force attack in which systematic checks are used to hack passwords until correct; the 'systematic' nature										

of this attack is repetition of which 1000s of attempts can be made per minute and consider that only 23 people are needed to have a 50% chance of sharing the same birthday in a year. [note: the odds are in the favor of the attackers, so have a very unique login.]										
DDOS: A Distributed Denial-of-Service attack is the worst type because it aims to completely shut down a network or service of business.										
Insider: we hate to think about inside attacks, but these types are very real and occur by an individual authorized to access systems.										
AI-Powered: artificial intelligence (or machine learning) tools can be easily deployed and sit undetected all the while gathering data and 'learning' with the intent of malice.										
People: regardless of attack type, people are the perimeter of effective defense and therefore rate your team- or organizational-level ability to work with one another on cyber defense and their ability to execute technology well and follow standard operating procedures of defense. [note: in other words, score your overall sense of people, process, and technology readiness for defense.]										
Total: Add the items in each vertical column and note the total in the corresponding cells here.										**Total Score: _____**

Scores 10-18 denote a low level of maturity and preparedness. If your score is in this range, leverage industry best practices to immediately implement cyber risk awareness campaigns and establish cyber policies and standard operating procedures for all employees.

Scores 19-25 denote a medium level of maturity and preparedness. If your score is in this range, congratulations, you have solid practices in place, but there is room for improvement. Connect with peers and collaborate on next-level practices for improved cyber maturity and readiness.

Scores 25-30 denote a high level of maturity and preparedness. Very well done. You have people, processes, and technology in place to mitigate cyber risk. This certainly does not mean you are immune to threat or a cyber-attack. So, remain vigilant and implement continual improvement practices and share lessons learned throughout your ecosystem.