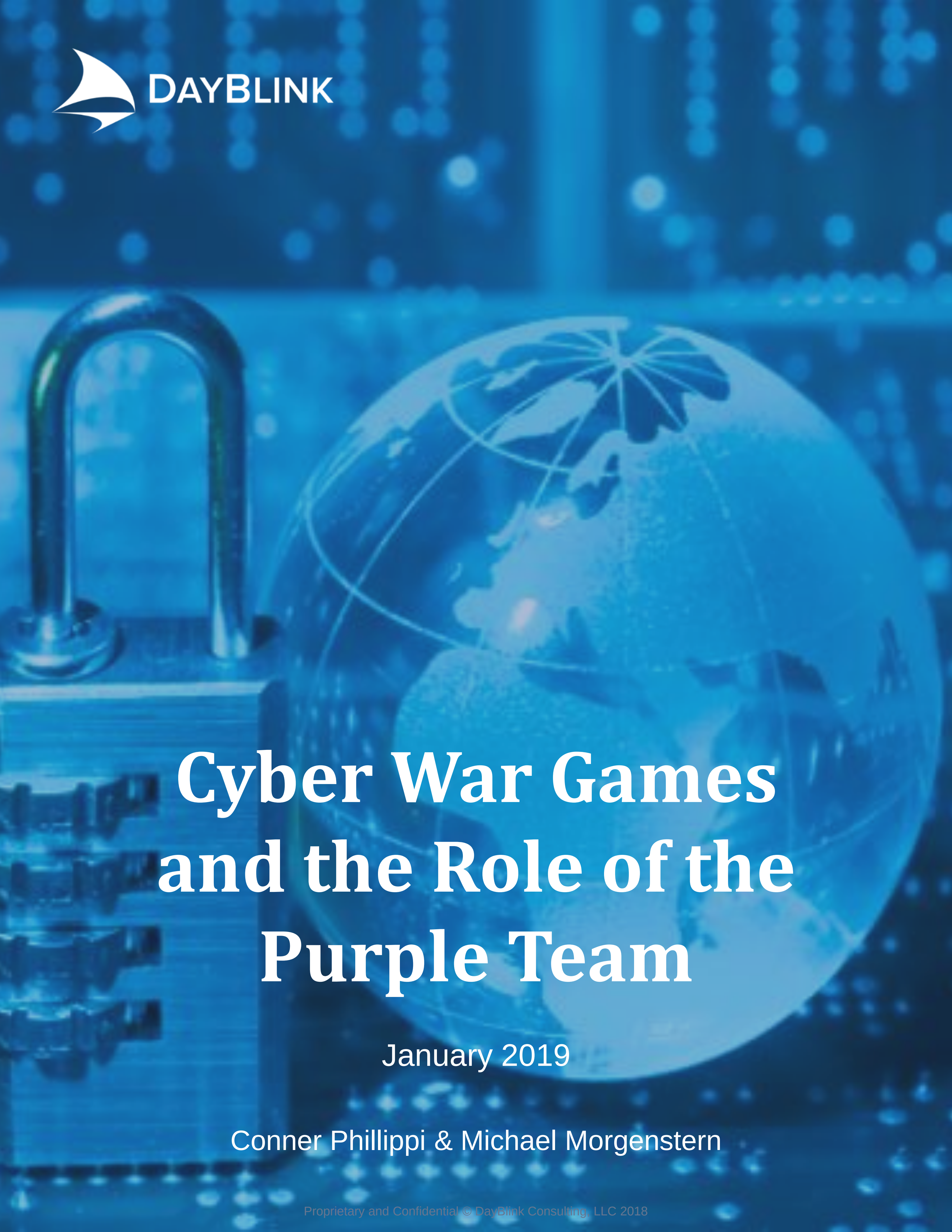


Cyber War Games and the Role of the Purple Team

January 2019

Conner Phillippi & Michael Morgenstern

INTRODUCTION

War Game Significance and Blue & Red Team Recap

With the continuous emergence of new cybersecurity threats, organizations across all industries are striving to modernize their defenses and bolster cyber resiliency. One of the leading research firms Cybersecurity Ventures forecasts that cyber crime damage will cost the world $6 trillion annually by 2021, doubling from $3 trillion in 2015[1]. Organizations can no longer ignore and reject the risks associated with cyber crime – the potential tangible and intangible damages are too high. Consequently, they must follow a variety of cybersecurity best practices including: implementing and updating related policies and procedures, assessing and remediating vulnerabilities nearly continuously, training information security (InfoSec) employees, and promoting organizational cyber awareness to safeguard assets and systems.

While these cybersecurity functions and activities are necessary, the ability to detect and respond to real cyber and physical attacks, isolate breaches, and communicate incidents to stakeholders remains heavily untested for most companies, which can be quite costly and could even result in bankruptcy. According to a recent study by the National Cyber Security Alliance, approximately 60% of hacked small and medium-sized businesses fail after six months[2]. Larger businesses can face significant brand impact, loss of intellectual property and private data, and multi-million dollar fines from regulators. To best prepare for cyber attacks and minimize their impact, organizations across all industries are increasingly turning to war games. Through these

Classic Team Definitions

Red Team
A group (internal or external) that emulates the behaviors and attack techniques of real-world attackers (hacktivists, governments, terrorist & criminal organizations, etc.) to test the effectiveness of an organization's cybersecurity posture

Blue Team
An internal group that defends an organization from internal and external threats, analyzes information systems to ensure security, identifies security flaws, verifies the effectiveness of each security measure, and makes certain all security measures will continue to be effective in the future

[1] "Cybercrime Damages $6 Trillion by 2021." Cybersecurity Ventures. May 14, 2018. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
[2] "America's Small Businesses Must Take Online Security More Seriously." Digital image. Nextgov. October 2012. https://www.nextgov.com/media/gbc/docs/pdfs_edit/050317jm1.pdf.

exercises, they assess and improve their cybersecurity posture and operational resiliency against a variety of different pressures and circumstances. During war games, organizations often use external Red Teams to attack and assess their systems and assets through real-life scenarios. During the attack, the organization’s internal InfoSec team (or a subset designated the Blue Team) responds to the Red Team’s assaults and attempts to maintain confidentiality, integrity, and availability across all systems and processes.

The Purple Team: War Game Facilitator and Project Manager

War games are difficult to perfect. Across war game exercises (assisting both Red and Blue Teams), several issues may exist between the Red and Blue Teams that hinder game effectiveness. More often than not, a tremendous gap exists in the communication between both the teams and InfoSec management, as there are no formal communication channels in place. Additionally, organizations that attempt to take on the Project Management Office (PMO) role often are overwhelmed or have misaligned priorities, which can have a drastic impact on war game and conclusion integrity. For example, InfoSec management that also acts as the PMO may unknowingly develop one-sided key performance indicators (KPIs) that make the Blue Team seem more effective than their actual security posture. Ineffective metrics combined with poor communication makes it extremely difficult for the organization to develop meaningful recommendations that can be implemented into the organization.

In order to maximize Red-Blue Team effectiveness, organizations have begun inserting a 3rd party PMO (or *Purple Team*) to facilitate the war game exercise and enable Red and Blue teams to focus solely on their assigned exercise goals and objectives without being burdened by administration. Figure 1 on the following page shows an abridged list of vital Purple Team war game roles:

Figure 1: Purple Team War Game Roles and Responsibilities

Scope Management

- Manage war game logistics, resources, and training materials
- Assign exercise action items for participants and establish deadlines
- Develop goals and objectives to provide direction to exercise participants
- Establish desired war game outcomes for the Blue Team and InfoSec

Documentation

- Analyze aspects of planning preceding exercise execution
- Note events and participants' corresponding actions during the exercise
- Organize feedback from all exercise participants and stakeholders
- Create After Action Report to discuss findings and lessons learned

Design and Development

- Select the war game scenario and type to emulate for the exercise
- Develop injects (events and incidents) to form the scenario's script
- Provide nontechnical insight and coordinate with system architects
- Create the Gamebook to serve as the master scenario event list (MSEL)

Evaluation

- Develop business-led KPIs (detection time, knowledge growth, etc.)
- Send surveys and post-exercise questionnaires to involved parties
- Conduct exit interviews to align outcomes with stakeholder commentary
- Consult research teams and SMEs for expertise & informed opinions

Facilitation

- Execute the war game exercise upon approval from leadership
- Collect exercise data via various mediums (logs, time stamps, etc.)
- Moderate workshops to foster knowledge transfer among participants
- Debrief participants/stakeholders via hot washes upon game conclusion

Corporate Education

- Publish recommendations and implement into a ticketing system
- Store lessons learned & AARs in a knowledge management system
- Develop war game newsletters for employees outside of InfoSec
- Hold strategy meetings with leadership to discuss war game implications

Relationship Management

- Foster a relationship of trust with PMO/leadership prior to exercise start
- Build rapport among Blue and Red Team members within exercise
- Establish ethos with stakeholders & SMEs throughout game lifecycle
- Coordinate an appropriate interrelationship among all parties

Future State Development

- Develop a post-exercise roadmap to improve cybersecurity posturing
- Identify and prioritize areas for improvement for the BT and InfoSec
- Create and/or mature necessary InfoSec processes and procedures
- Establish timeline and dates for future war game exercises

All of the aforementioned Purple Team functions maximize value for game participants, management, and the organization as a whole. Game participants can focus solely on their relevant functions within a tailored war game exercise, management can avoid conflicts of interests while understanding areas of InfoSec improvement through business-led KPIs, and the organization can continually grow its cybersecurity defenses by the Purple Team's corporate education training and post-exercise recommendations.

PURPOSE OF WAR GAMES

War Games Provide Valuable Insight to Management

Unlike penetration tests which typically identify solely technical vulnerabilities, war games leverage actual business scenarios that are relentless and unforgiving (and at times controversial) to authentically simulate realism and effectively test an organization's cyber defenses. Upon conclusion of a Live war game exercise, the Purple Team should provide management insight across the following managerial metrics at minimum:

- Degree of overall organizational cybersecurity maturity and posture
- Degree of transparency and communication across management and the Blue Team
- Effectiveness of current cybersecurity policy and procedures
- Effectiveness of ongoing and previous cybersecurity training
- Effectiveness of tested security controls in place
- Level of Blue Team / InfoSec incident response preparedness
- Level of Blue Team intercommunication and chemistry
- Level of Blue Team exercise-related knowledge growth
- Level of security / protection of tested corporate assets and potential damages upon exploitation
- Severity of technical and human vulnerabilities related to tested corporate assets

Ultimately, the organization should incorporate the Purple Team's findings and lessons from war game exercises to understand gaps in their defenses, improve their cybersecurity posture, and reduce the probability of similar attacks being successful in the future by actual assailants.

War Games are a Form of Risk Mitigation

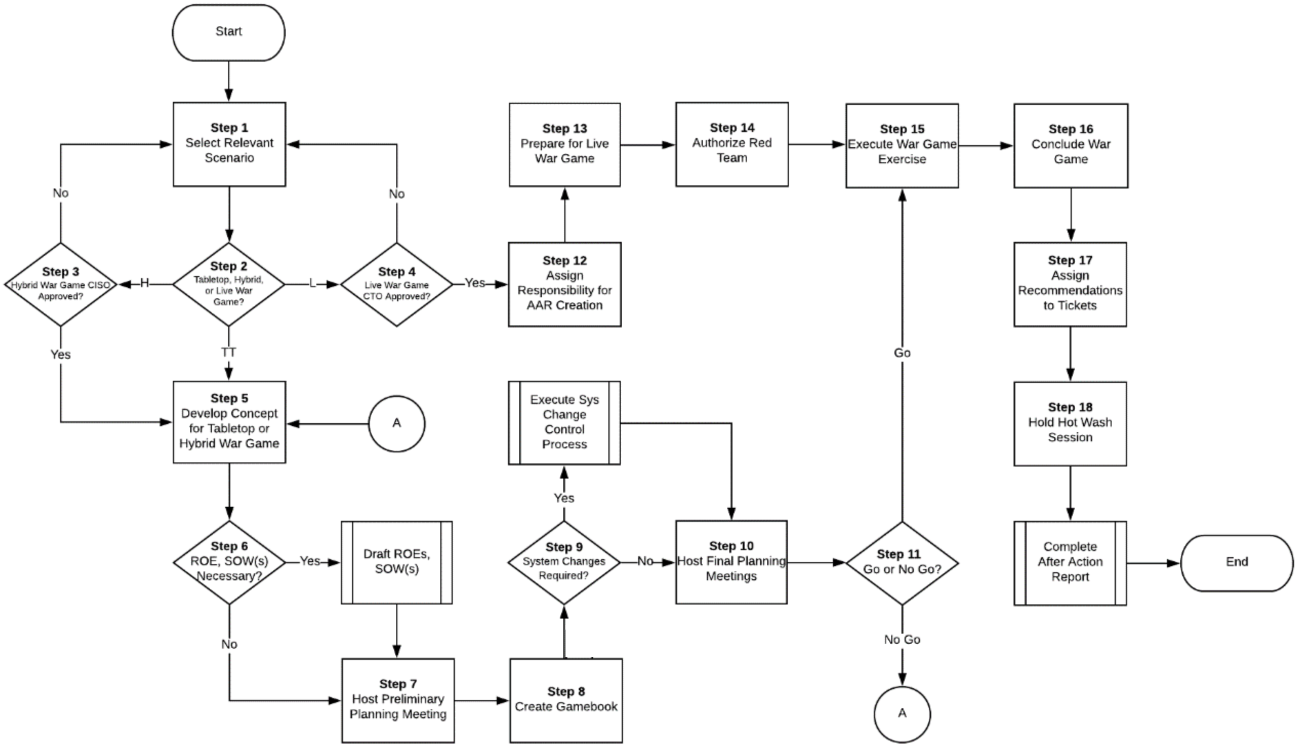
The growing presence of data protection regulations such as GDPR, HIPAA, and PCI DSS coupled with high privacy expectations from consumers and lawmakers have forced companies to implement a wide range of technical, operational, and managerial security controls to minimize the risk of breaches. Although vulnerabilities are impossible to entirely eradicate, it is a company's responsibility to minimize the risk of customer PII/PHI sensitive proprietary data exposure and outright theft by identifying and prioritizing vulnerability remediation. Currently, 80% of all businesses conduct security assessments and/or penetration testing to identify vulnerabilities and weaknesses[3]; however, some surveys show that 90% percent of U.S. business have had a cybersecurity incident in the past year[4]. It is apparent that even after companies conduct internal and external penetration tests, their corporate assets and systems remain vulnerable to a wide variety of threats and attacks. Additionally, even after being hacked, 46% of businesses fail to change their security strategy[5]. Penetration tests do not provide advice on organizational and strategic change -- they simply offer insight into the current vulnerability state of an organization. In this modern era of advanced persistent threats, companies need to leverage war games to properly test their organization's defenses against attacks from real world threat agents that no penetration test can effectively simulate.

WAR GAME PLANNING

Once an organization decides to conduct a war game, an executive such as the CEO, CTO, CIO, CISO or Blue Team lead typically first contacts consultant(s), who assumes the role of the Purple Team (PMO), to facilitate the war game. Relevant company executives and senior management will form the Game Committee overseeing the Purple Team throughout the entire engagement. The Purple Team must present logical steps for breaking out war game operations to the Game Committee to align on needs, process, and flow as shown on the following page:

[3] "New Report Shows That One in Five Businesses Don't Test for Security Vulnerabilities." Trustwave. September 14, 2016. https://www.trustwave.com/Company/Newsroom/News/New-Report-Shows-that-One-in-Five-Businesses-Don-t-Test-for-Security-Vulnerabilities/.
[4] "HSB Cyber Study Shows 90 Percent of Businesses Experienced Hacking Incidents in the Last Year." Munichre.com. May 17, 2016. https://www.munichre.com/HSB/cyber-survey-2016/index.html.
[5] "Survey: 46 Percent of Organizations Fail to Change Security Strategy After a Cyber Attack." BusinessWire. February 28, 2018. https://www.businesswire.com/news/home/20180228005275/en/Survey-46-Percent-Organizations-Fail-Change-Security.

Figure 2: War Game Process Flow


Start
Step 1 Select Relevant Scenario
No
No
Step 3 Hybrid War Game CISO Approved?
H
Step 2 Tabletop, Hybrid, or Live War Game?
L
Step 4 Live War Game CTO Approved?
Yes
Yes
TT
Step 5 Develop Concept for Tabletop or Hybrid War Game
A
Step 6 ROE, SOW(s) Necessary?
Yes
Draft ROEs, SOW(s)
No
Step 7 Host Preliminary Planning Meeting
Step 8 Create Gamebook
Step 9 System Changes Required?
Yes
Execute Sys Change Control Process
No
Step 10 Host Final Planning Meetings
Step 11 Go or No Go?
Go
No Go
A
Step 12 Assign Responsibility for AAR Creation
Step 13 Prepare for Live War Game
Step 14 Authorize Red Team
Step 15 Execute War Game Exercise
Step 16 Conclude War Game
Step 17 Assign Recommendations to Tickets
Step 18 Hold Hot Wash Session
Complete After Action Report
End

Selecting the Right War Game Scenario

Purple Teams typically work with Red Teams and Risk Management Teams to prioritize InfoSec (Blue Team) capabilities for testing and improvement based upon the associated risk for the organization and its stakeholders. Stakeholder teams should determine which high risk and/or immature capabilities are most suitable for testing in a war game exercise (some capabilities are better off tested through formal training and instruction rather than war gaming). After identifying capabilities for testing, the Purple Team and Gaming Committee select the most applicable war game scenario to improve the chosen Blue Team capabilities (note: competent Purple Teams should have an arsenal of premade war game scenarios available for selection.) Every potential scenario can be characterized by a variety of different elements such as stage in the Lockheed Martin Cyber Kill-Chain, actor, target, method, desired asset, tested defense, and outcome as shown in Figure 3:

Figure 3: War Game Elements

Cyber Kill-Chain
The actor's malicious action(s)

Reconnaissance
Harvesting email addresses, conference info. etc.

Weaponization
Coupling exploit with backdoor into deliverable payload

Delivery
Delivering weaponized bundle to the victim via email web, USB, etc.

Exploitation
Exploiting a vulnerability to execute code on a victim's system

Installation
Installing malware on an asset

Command & Control
Command channel for remote manipulation of victim

Actions on Objectives
With "Hands on Keyboard" access, intruders accomplish their goals

Actor
The antagonist or aggressor of the war game

3rd Party	Nation-State
Criminal Organization	Organization
Hacktivist	Unknown Actor
Insider	

Target
The asset targeted by the actor

3rd Party	Mobile Phone
Administrator Account	Networking Hardware
Clientele	PII/PHI
Computer	Private/Public Network
Corporate Confidential Info.	Security Device
Credential	Sensitive Document
Employee	Server
Internet Traffic	Social Media Account
IoT	Website

Method
The practice or tool used by the actor

Code Injection	Password Attack
DDoS & DoS	Security Question Manipulation
Insider Activity	Skimming
Malware	Social Engineering
Man-in-the-Middle Technique	Theft
Networking	Unauthorized Physical Access

Desired Asset
The sought after asset

Account Access	Monetary Gain
Administrator Account	Personally Identifiable Info.
Corporate Confidential Info.	Protected Health Info.
Credentials	Traffic Redirection Capability

Tested Defense
The defense tested by the attack

Access Management	Decryption Capability
Anti-Malware	Employee Vigilance
Cellular Infrastructure	Network Security
Corporate Policy	Password Management
DDoS & DoS Protection	Website Security

Outcome
The tangible consequences of the attack

Account Hijacked	Key Stolen
Asset Exploitation	Monetary Loss
Data Destroyed	PII / PHI Stolen
Data Stolen	Service Downtime
Harmed Reputation	Vandalism
Intercepted Communication	

The identified capabilities should be mapped to a variety of elements that make up different games within the Purple Team's game arsenal to identify the most appropriate game. Figure 4 on the next page includes an excerpt of a sample war game arsenal:

[6]"The Cyber Kill Chain." Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Figure 4: War Game Scenario

War Game Name	Kill-Chain Stage	Actor	Target	Method	Desired Asset	Tested Defense	Outcome

[redacted]	●○○○○○○	Organized Crime	Employee; Mobile Phone;
			Server
				Social Engineering;
				Networking
					Corporate Confidential Info.	Employee Vigilance;
						Corporate Policy;
						Network Security
							Data Stolen

[redacted]	●○○○○○○	Organization	Private Network;
			Networking Hardware;
			Server
				Networking;
				DoS
					Personal Health Info.	Network Security;
						Corporate Policy
							Unknown

[redacted]	●○○○○○○	Hacktivist	Website; Employees	Networking; Code Injection; Social Engineering	Corporate Confidential Info. Personally Identifiable Info.	Corporate Policy	Data Stolen
[redacted]	●○○○○○○	Nation-State	Employees; Mobile Phones; Mobile Data Traffic	Man-in-the-Middle Attacks	Corporate Confidential Info.	Cellular Infrastructure; Corporate Policy	Intercepted Communications
[redacted]	●○○○○○○	Organized Crime	Computers; Private Network; Social Media Accounts	Man-in-the-Middle Attack;	Credentials; Corporate Confidential Info.	Corporate Policy	Account Hijacked; Data Stolen

[redacted]	○●○○○○○	Organized Crime	Employee;
			Computer;
			Corporate Confidential Info.
				Password Attack;
				Theft
					Monetary Gain	Password Management;
						Corporate Policy
							Data Stolen

[redacted]	○●○○○○○	Hacktivist	IoT	Networking; Unauthorized Physical Access	Unknown	Network Security; Physical Security	Infected/Exploited Assets

[redacted]	○○●○○○○	Organized Crime	Employees;
			Computers
				Social Engineering;
				Malware
					Personally Identifiable Info.	Employee Vigilance;
						Anti-Malware
						Corporate Policy;
							Personal Identifiable Info. Leaked

[redacted]	○○●○○○○	Hacktivist	Employee;
			Mobile Phone
				Social Engineering;
				Malware
					Corporate Confidential Info.	Employee Vigilance;
						Corporate Policy;
						Anti-Malware
							Personal Identifiable Info. Leaked

[redacted]	○○●○○○○	Hacktivist	Employees;
			Computers;
			Networks;
			Credentials
				Social Engineering;
				Malware;
				Main-in-the-Middle Attack
					Corporate Confidential Info.	Corporate Policy;
						Anti-Malware
							Data Stolen

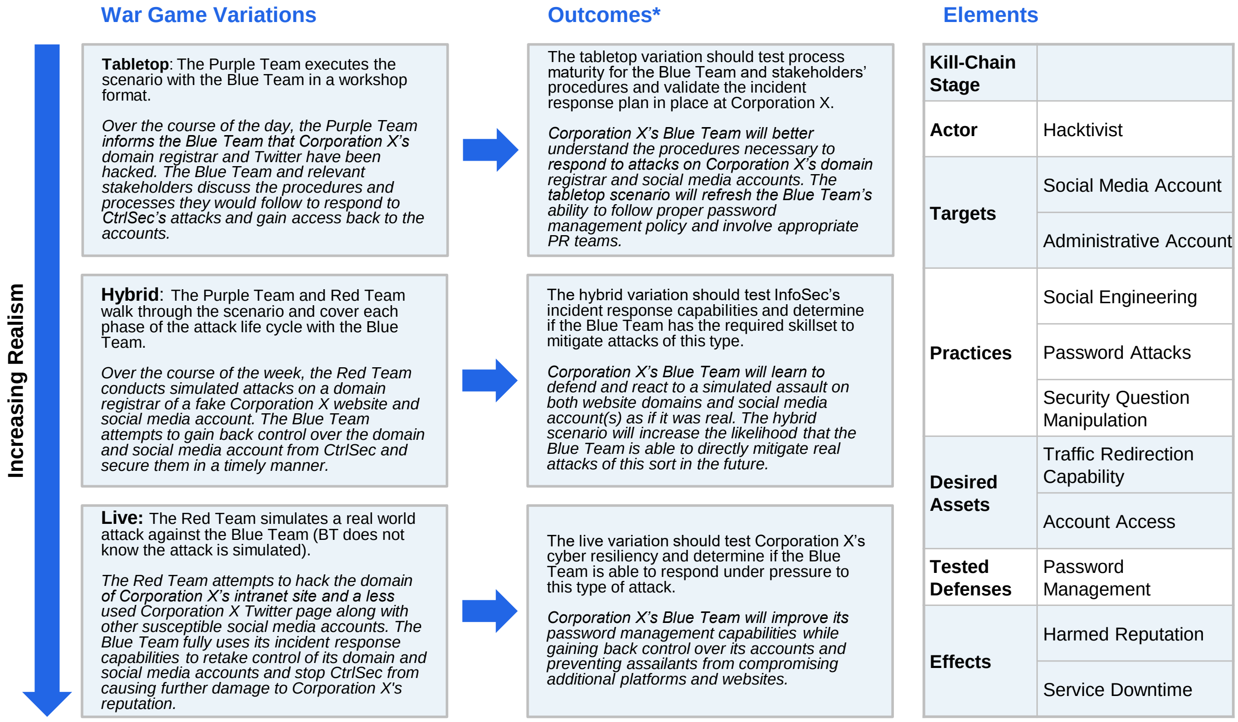
[redacted]	○○○●○○○	Insider	Unknown	Insider Activity; Theft	Corporate Confidential Info.	Access Management	Data Stolen
[redacted]	○○○●○○○	Unknown Actor	Servers	Networking	Corporate Confidential Info.	Network Security	Data Stolen
[redacted]	○○○●●○○	Hacktivists	Servers; Private Network	DDoS; Malware	Admin. Account	DDoS Protection; Network Security	Service Downtime; Key Stolen

Example War Game Scenario

As an example, assume that the chosen capabilities indicate that the organization should test incident response speed, social engineering protection, and password security for Marketing-related assets. An appropriate war game could test the Blue Team's incident response effectiveness after discovering a website compromise by a hacktivist group that leveraged social engineering and password attack techniques to compromise various internet accounts and websites, potentially damaging corporate relations with consumers.

Figure 5: War Game Scenario

***Scenario Description:** A hacktivist group called CtrlSec wants to put all visitors to Corporation X's website in for a special treat. CtrlSec has hacked into their domain registrar and redirected website traffic to a very inappropriate website. Additionally, Corporation X's Twitter account is tweeting its own web address and #CtrlSec with promises of additional attacks on other Corporation X-related social media platforms and websites in the upcoming days.*



War Game Variations

Tabletop: The Purple Team executes the scenario with the Blue Team in a workshop format.

Over the course of the day, the Purple Team informs the Blue Team that Corporation X's domain registrar and Twitter have been hacked. The Blue Team and relevant stakeholders discuss the procedures and processes they would follow to respond to CtrlSec's attacks and gain access back to the accounts.

Hybrid: The Purple Team and Red Team walk through the scenario and cover each phase of the attack life cycle with the Blue Team.

Over the course of the week, the Red Team conducts simulated attacks on a domain registrar of a fake Corporation X website and social media account. The Blue Team attempts to gain back control over the domain and social media account from CtrlSec and secure them in a timely manner.

Live: The Red Team simulates a real world attack against the Blue Team (BT does not know the attack is simulated).

The Red Team attempts to hack the domain of Corporation X's intranet site and a less used Corporation X Twitter page along with other susceptible social media accounts. The Blue Team fully uses its incident response capabilities to retake control of its domain and social media accounts and stop CtrlSec from causing further damage to Corporation X's reputation.

Outcomes*

The tabletop variation should test process maturity for the Blue Team and stakeholders' procedures and validate the incident response plan in place at Corporation X.

Corporation X's Blue Team will better understand the procedures necessary to respond to attacks on Corporation X's domain registrar and social media accounts. The tabletop scenario will refresh the Blue Team's ability to follow proper password management policy and involve appropriate PR teams.

The hybrid variation should test InfoSec's incident response capabilities and determine if the Blue Team has the required skillset to mitigate attacks of this type.

Corporation X's Blue Team will learn to defend and react to a simulated assault on both website domains and social media account(s) as if it was real. The hybrid scenario will increase the likelihood that the Blue Team is able to directly mitigate real attacks of this sort in the future.

The live variation should test Corporation X's cyber resiliency and determine if the Blue Team is able to respond under pressure to this type of attack.

Corporation X's Blue Team will improve its password management capabilities while gaining back control over its accounts and preventing assailants from compromising additional platforms and websites.

Elements

Kill-Chain Stage	
Actor	Hacktivist
Targets	Social Media Account
	Administrative Account
Practices	Social Engineering
	Password Attacks
	Security Question Manipulation
Desired Assets	Traffic Redirection Capability
	Account Access
Tested Defenses	Password Management
Effects	Harmed Reputation
	Service Downtime

Impacted Stakeholders

CTO, CISO, InfoSec, Head of Incident Response, Public Relations Department, Website Customers and Followers

*Outcomes should be changed/modified during the planning of each war game exercise based upon the goals of the Purple Team and other relevant stakeholders

As demonstrated in Figure 5, war games are able to be executed in three different variations with consequent outcomes. Expected outcomes should be predetermined by the Purple Team and Game Committee; however, the actual outcome may be different depending on the Blue Team's game performance.

Determining the Most Suitable War Game Variation

Tabletop exercises also known as Workshops consist of the Blue Team and other stakeholders discussing the processes and procedures they would follow to respond to a specific incident. During Hybrid exercises, the Purple Team and Red Team discuss the scenario and cover each stage of the attack lifecycle with the Blue Team, usually demonstrating particular attacks. Lastly, in a Live exercise, the Red Team simulates a real world attack against the Blue Team, whom would not be aware of the plan beforehand. Generally, only the CEO, CTO or CIO, and an additional executive will know about a Live simulation to ensure the external Red Team is treated as a real threat. Additionally, Purple Teams typically contract an external Red Team to assist with game execution unless the organization specifically maintains their own internal Red Team or offensive engineering group.

The organization’s current cybersecurity posture influences which variation is most appropriate. Without baseline policies and procedures in place, not even tabletop exercises (the least involved type of war game) would be useful or successful. Organizations should first ensure that all relevant processes and documentation are well-established before moving on to more advanced hybrid and live exercises.

WAR GAME CONSTRUCTION AND EXECUTION

The steps of war game planning depend heavily on the war game variation: Tabletop, Hybrid, or Live.

Tabletop and Hybrid Game Development

For a Tabletop or Hybrid war game, the Purple Team should receive full approval from the CISO before developing the concept of the war game. If any previous war games have been conducted, it’s critical to review the lessons learned to ensure measures are in place to avoid duplicative mistakes. The Purple Team and Gaming Committee should jointly define goals and objectives of the Blue Team that test the chosen processes and capabilities through the lifecycle of the war game. Additionally, the Purple Team should identify external participants (Red Teams, SMEs, and external organizations), arrange logistical needs (transport, lodging, and security), develop training materials (policies, procedures, and technical guides) and provide resources (training environments, personnel, etc.) for the engagement. Next, the Purple Team should ensure that Rules of Engagement and additional contractors are in place (e.g. Red Teams, SMEs, etc.). The Purple Team and potential experts should review the war game exercise with the Red Team to create a war game Gamebook, which contains detailed exhibits and scripts that expand upon the initially selected war game scenario. War game exhibits should specify actual planned occurrences within the script in order to drive the war game. Internal and external participants (excluding the Blue Team) should collaborate to draft appropriate injects for the war game exercise. The script should drive the objectives and goals of the exercise; however, the scripted events must also consider the capabilities of the Blue Team and Red Team and anticipate operational risk (e.g. accidentally releasing malware into a real IT environment). Only after the Gaming Committee and the CISO are comfortable with the war game plan, should they authorize the execution of the war game.

Live Game Development

For live games, the Purple Team should receive full approval from the CTO, CIO, or an individual in a similar position before moving forward. Once approval has been received, a Red Team (best if contracted by the Purple Team) that is capable of carrying out the desired Live war game exercise should be onboarded (including signing non-disclosure documents) and briefed on the relevant Rules of Engagement. Red Teams typically spend some time familiarizing themselves with the organization’s infrastructure to prepare for the war game. The Red Team should begin to identify potential network and physical entry points as well as aggregate potential targets on corporate systems and assets. Additionally, the Red Team needs to be cautious about accessing certain sets of data or causing permanent harm to assets, as legal repercussions could ensue. Importantly, a Purple team could provide data copies, or cordoned off environments, without alerting the Blue Team.

Executing War Games

For Tabletop exercises, the Blue Team head will typically initiate the war game. The Purple team begins to use IR injects over the course of a day to challenge Blue Team and stakeholder processes and procedures. For hybrid war games, the Purple Team and Red Team walk through the attack scenario and cover each phase of the attack lifecycle. For live war games, the Red Team should be authorized by the CEO, CTO, or CIO to begin its "real" attack on the organization and proceeds to simulate a real world attack on the organization.

Purple Team facilitation and moderation should vary depending on the type of exercise. Tabletops are often completely hands on, whereas live war games could be fully hands off (only KPIs will be tracked). Regardless, dedicated war game observers should collect observations and feedback and note findings throughout the game by the means of real-time observation and monitoring via software, cameras, and in-person observation.

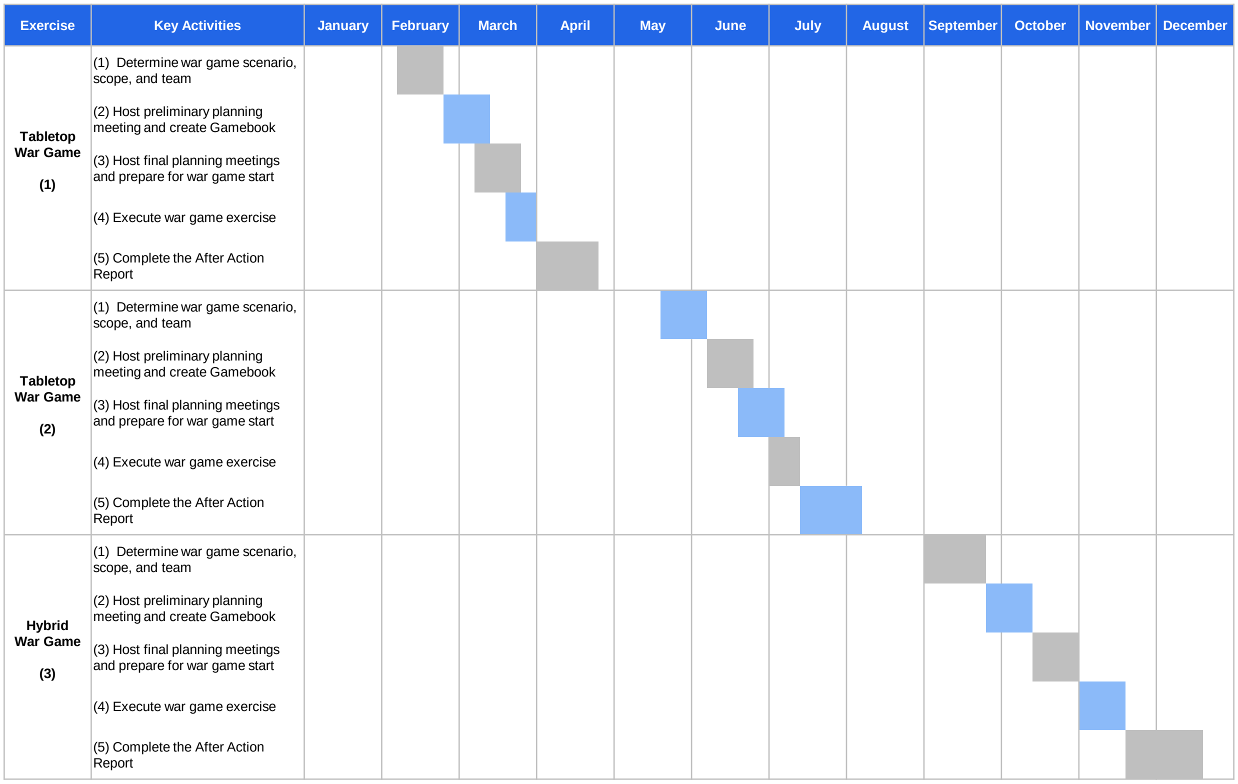
War Games Results and After Action Analysis

Commonly, war games typically end with the expectation that all parties have learned something. Red Teams often record and then provide their attack methods to the Blue Team. In practice, those findings get added to the backlog of vulnerabilities, essentially relegating the war game exercise to a sophisticated penetration test. But there is a far better approach.

After the war game has concluded, the Purple Team should debrief stakeholders to confirm what actually occurred in each stage of the exercise and ensure mutual alignment. For live exercises specifically, the Purple Team should facilitate information sharing workshops and hot wash sessions to allow discussion between the Blue and Red Teams and identify areas of both success and improvement. In general, post-exercise questionnaires and surveys are commonly used to gather information from participants. Data points such as timestamps specifying when certain actions took place, written messages throughout the exercise, unit activity journals, function and position checklists, platform, tool, software, and team chat logs, audio conference minutes, and periodic status reports should all be collected and synthesized. Based on findings made during the exercise, the Purple Team should develop recommendations for future war game projects and implement them into a ticketing system within a knowledge management system. This enables recommendations to be referenced prior to future war games. After the exercise has concluded, the Purple Team should develop a written after action report detailing exercise observations, findings, recommendations, and areas for continuous improvement.

Clients typically recognize the need to repeat the war game process to continuously test their defenses. Sophisticated InfoSec organizations generally manage a schedule like this:

Figure 6: War Game Scheduling



Exercise	Key Activities	January	February	March	April	May	June	July	August	September	October	November	December
Tabletop War Game (1)	(1) Determine war game scenario, scope, and team		▨										
	(2) Host preliminary planning meeting and create Gamebook		🟦	🟦									
	(3) Host final planning meetings and prepare for war game start			▨									
	(4) Execute war game exercise			🟦									
	(5) Complete the After Action Report				▨								
Tabletop War Game (2)	(1) Determine war game scenario, scope, and team					🟦	🟦						
	(2) Host preliminary planning meeting and create Gamebook						▨						
	(3) Host final planning meetings and prepare for war game start						🟦	🟦					
	(4) Execute war game exercise							▨					
	(5) Complete the After Action Report							🟦	🟦				
Hybrid War Game (3)	(1) Determine war game scenario, scope, and team									▨			
	(2) Host preliminary planning meeting and create Gamebook									🟦	🟦		
	(3) Host final planning meetings and prepare for war game start										▨		
	(4) Execute war game exercise											🟦	
	(5) Complete the After Action Report											▨	▨

FINAL THOUGHTS

Organizations cannot afford to ignore risks associated with cybersecurity due to the potential for high costs or fines and lasting intangible brand damage. To combat cybersecurity risk, organizations should continuously engage in passive penetration testing to identify technical vulnerabilities existing within assets and security controls. Simultaneously, it is critical to layer on active war games on top of penetration tests to authentically test and improve Blue Team / InfoSec incident response to real cyber and physical attacks, breach isolation, and incident communication to stakeholders.

While organizations can use an internal PMO team to facilitate war game execution, Blue Team KPI bias, immature communication channels, misaligned priorities, lack of expertise, and administrative burden can derail war games and call game conclusion integrity into question. Businesses should strongly considering hiring a Purple Team, as having to run an additional war game due to questionable results can be costly use of resources and security personnel.

Prior to running a war game, organizations should consider what assets are of the greatest risk to attack and assess their cybersecurity maturity to determine if a Tabletop, Hybrid, Live war game is most appropriate. After the war game has been run, it is critical that the Purple Team takes some time to digest what occurred during the game through the means of surveys, interviews, team notes, and systems datapoints to best present valuable findings and recommendations to InfoSec management with the ultimate goal of improving cyber resiliency.

ABOUT THE AUTHORS

Conner Phillippi, Associate of (ISC)2, is an Analyst within DayBlink's cybersecurity Center of Excellence and is based in the Vienna, Virginia office.

Michael Morgenstern is a Partner and Practice Lead of DayBlink Consulting's cybersecurity Center of Excellence, a former cybersecurity entrepreneur, and is based in the Vienna, Virginia office.

Please direct questions and comments about this report to cyber@dayblink.com

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents.

The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

DAYBLINK

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cyber@dayblink.com
Call: 1 (866) 281-4403