Cyber Wargaming: Lessons Learned Influencing Security Stakeholders

Abstract

Our world faces numerous challenges related to cyber security, and they are increasing. These challenges include diversifying data breaches, deficit of cyber talent, lack of cyber skills in non-technical positions, issues in software and hardware product development, and specialization within cyber security itself. Promising solutions lay in the areas of Serious Gaming and wargaming, evidenced by SAIC's attack and defense cyber wargame which has been created in the last year. The wargame is fast-paced at 2.5 hours start to finish. The game architecture is realistic and isolated, steadily improving with each event, and shows surprisingly positive results across diverse stakeholder community. And, improvements are planned over the next year. This paper will describe all of this is in much more detail.

Cyber-Related Challenges Faced in all Industries

Cyber was hard in the past, requiring an understanding of technical vulnerability and human vulnerability. But given tremendous advancement in areas such as migration to Cloud Computing, maturation of the Internet of Things (IoT), and increasingly active and ambiguous threat actors, the challenge facing cyber security stakeholders is quite significant moving forward. The following challenges face our industry:

1. Data Breaches (as evidenced by Verizon's annual Data Breach Report[1] **shown in Figure 1**) show significant diversity in Pattern, Action, Asset spread across marketplace
2. There is a worldwide deficit of one million job openings[2], with demand expecting to increase to six million by 2019.
3. Many activities that affect security are performed by people that don't understand security. Knowledge in non-tech positions such as executive

Figure 1 - Examination of Verizon 2017 Data Breach Report Shows Diverse and Increasingly Challenging Map of Patterns, Actions and Assets Defining Breaches Across Industries

[1] Verizon Data Breach Report, 2017, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[2] Cisco, "Mitigating the Cybersecurity Skills Shortage, 2015, http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

SAIC
Redefining Ingenuity™

management, finance, staffing, procurement and contracting are examples. One evolving form of fraud called "whaling"[3] is a typical impact.

4. There are increasing issues in technology product development related to lack of security in product design, or lack of security awareness in product development, delivery and support. One issue recently showing this is the recent raid by Ukrainian authorities on the accounting software maker MeDoc[4], reportedly a source of the NotPetya malware.
5. Specialization within Cyber itself can be a problem given the scale and depth of the cyber skills taxonomy (defined by the U.S. National Institute of Science and Technology through their National Cybersecurity Workforce Framework[5]), with some professionals not fully understanding the entire security spectrum, whereas others are more general in their understanding

Traditional Approaches

Cyber Security Training

Many organizations have invested in the past in cyber security training, both by sending staff to a training course, or bringing a training team in for internal delivery. However, this training is often oriented toward technical staff, and usually based on the goal of achieving some form of cyber security certification for participating students. This generally ignores many of the non-technical/non-cyber staff that would also benefit from training. In addition, even for those that attend cyber security training, traditional training techniques can represent issues[6] such as: boring content, lacking interaction, no measurement, scare-vs-teach, education not being security's core competency. Cyber Security Training can be much more effective if the audience is expanded, and the training delivery is made more dynamic.

Cyber Security Product Demonstration

Many organizations also invest significantly in acquiring information technology products and services to combat threats, minimize risk, and arm cyber security staff in addressing the challenges defined earlier. But this requires an effective process by which the vendor industry communicates product value and position products and services for an eventual sale and implementation. However, this interaction like training, tends to be briefing based, non-interactive, non-engaging and therefore do not compel audience to think and retain key messages. Cyber Security Products and Services can be communicated (and sold) much more effectively to customers if the demonstration is made more dynamic.

[3] CIO.com, 2016, "Whaling emerges as major cybersecurity threat", http://www.cio.com/article/3059621/security/whaling-emerges-as-major-cybersecurity-threat.html
[4] The Register, 2017, "Watch: Armed Ukrainian cyber-cops raid MeDoc in NotPetya probe", https://www.theregister.co.uk/2017/07/05/ukraine_authorities_raid_me_docs_in_notpetya_investigation/
[5] NIST, 2017, "National Initiative for Cybersecurity Education (NICE)", https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[6] Wombat Security, 2017, "Why Most Cyber Security Training Doesn't Work", https://www.wombatsecurity.com/about/news/why-most-cyber-security-training-doesnt-work

SAIC Redefining Ingenuity™

Influencing Approaches

Serious Gaming

Serious gaming offers an interesting evolution in industry for the use of gaming as the platform for training and/or demonstration. A definition:

> *A **SERIOUS GAME** OR **APPLIED GAME** IS A GAME DESIGNED FOR A PRIMARY PURPOSE OTHER THAN PURE ENTERTAINMENT…THE IDEA SHARES ASPECTS WITH SIMULATION GENERALLY, INCLUDING FLIGHT SIMULATION AND MEDICAL SIMULATION, BUT EXPLICITLY EMPHASIZES THE ADDED PEDAGOGICAL VALUE OF FUN AND COMPETITION*[7]

While gaming can be considered a hobby to some, the last part of this definition is significant. The "fun and competition" aspect makes serious gaming a compelling medium for capturing the attention of the student and/or customer audience. Most will agree that the more compelling and interactive the training/presentation, the more engaged the audience will be.

Military Wargaming

Similarly, "wargaming" offers platform and approach that compels participants. A definition:

> *A WARGAME (ALSO WAR GAME) IS A STRATEGY GAME THAT DEALS WITH MILITARY OPERATIONS OF VARIOUS TYPES, REAL OR FICTIONAL. WARGAMING IS THE HOBBY DEDICATED TO THE PLAY OF SUCH GAMES, WHICH CAN ALSO BE CALLED CONFLICT SIMULATIONS, OR CONSIMS FOR SHORT. WHEN USED PROFESSIONALLY BY THE MILITARY TO STUDY WARFARE, "WAR GAME" MAY REFER TO A SIMPLE THEORETICAL STUDY OR A FULL-SCALE MILITARY EXERCISE.*

The use of wargaming by nation state military organizations has long been held as critical for preparing participants for actual warfare. A recent example of wargaming is **shown in Figure 2**, where realistic conditions are provided to a large and diverse set of participants.

Figure 2 - U.S. Army Soldiers acting as Observer Controller Trainers watch as Ukrainian soldiers react to enemy fire at an entry control point during exercise Rapid Trident 16 July 5, 2016. The exercise is a regional command post and field training exercise that involves about 2,000 Soldiers from 13 different (U.S. Army photo by Sgt. 1st Class Whitney Hughes/Released)

[7] https://en.wikipedia.org/wiki/Serious_game

SAIC Cyber Wargame

SAIC over the past year has combined serious gaming and wargaming into a realistic cyber wargaming environment that positions participants at computers to experience how cyber-attack and defense are planned, delivered and executed. The wargame scenario includes three teams: an attacking team (hacktivist oriented), another attacking team (nation state oriented), and a defending team (hybrid government-industrial infrastructure oriented). The defending team defends an array of Information Technology (IT) and Operational Technology (OT) assets including public facing web/database server, IT workstation, and an emulated critical infrastructure plant. Target assets are located on different networks, with a combination of standard IT protocols as well as Industrial Control (Modbus/Transport Control Protocol - TCP) protocols. The defending team's main goal is to keep critical infrastructure operational while monitoring database and web server, while under duress. Having two attack teams gives participants the opportunity to role-play the different motivations, skillsets, and mentalities associated with an enemy Nation State or Hacktivist group. The Red teams also will have the capability to demonstrate how social engineering and leveraging an insider threat works. The wargame is scripted and scheduled to last 2.5 hours start to finish. The agenda, and part of a player-coaches script is **shown below, in Figure 3**. Teams, two attacking and one defending compete in parallel. Each team role-plays having different motivations, operational methodologies, responsibilities, assets and tools. And, game content is heavily influenced by real events (Stuxnet[8], HB Gary Federal[9]). Finally, the game uses industry best practice frameworks for cyber operations, both offensive[10] and defensive[11].

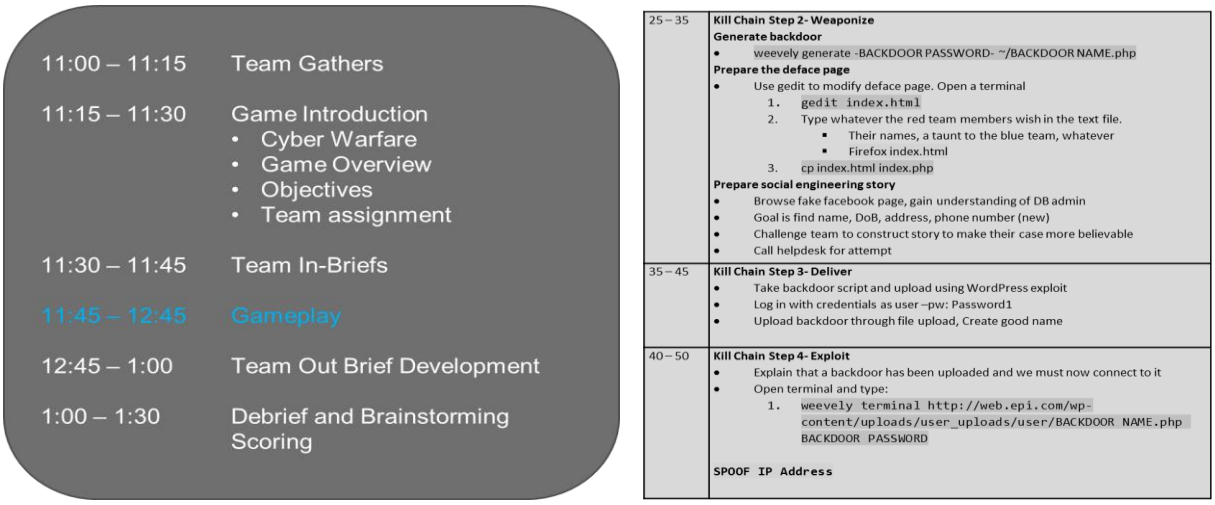

Figure 3 - Wargame is Fast-Paced at 2.5 Hours Start to Finish, Heavily Reliant on Game Scripts used by Player-Coaches

[8] Wired Magazine, Kim Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[9] Ars Technica, Peter Bright, "Anonymous speaks: the inside story of the HBGary hack", 2011, https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

[10] Lockheed Martin, 2017, Cyber Kill Chain, http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

[11] SAIC, 2017, Cyber Security Edge, https://www.saic.com/services-solutions/technology-solutions/cybersecurity

SAIC Redefining Ingenuity™

Game Architecture

The wargame environment is designed with an emphasis on off-the-shelf, freely-available, industry-standard tools and technologies, listed below. Our primary components which are **depicted below in Figure 4** include:

Game Component/Service
Virtualized platform using VMWare vSphere
pfSense Routing and Firewalls
Physical switches for laptop/remote connection to game environment
Attacker network mimics internet; Kali Linux used for most attacks
Multiple blue team networks emulating industrial corporation with segmentation
Modified open source emulation of oil refinery[12]
Modbus/TCP communications between Industrial Control interface and refinery
Vulnerable web, database and ftp servers (Ubuntu-based, WordPress, MySQL)
Attackers pivot from IT over to OT
Persistent environment located at SAIC Reston, VA iSpace lab
Separate roadshow environment which we take to conferences/remote locations
Visual depiction of network traffic using NexDefense Sophia

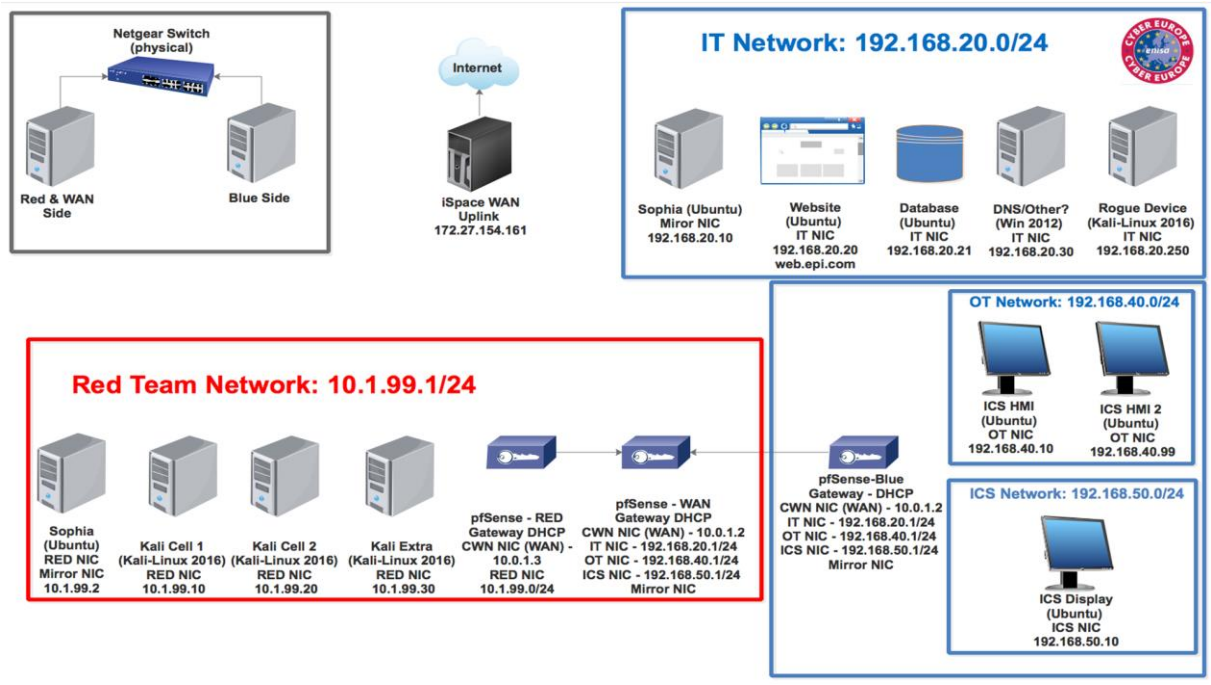

Figure 4 - Game Architecture Enables Virtual and Isolatable Game Environment Which Provides both Attack, Defense and Administrative Capability

[12] VirtuaPlant, Author: Jan Seidl, Forked and Enhanced by Justin Beale, https://github.com/jseidl/virtuaplant

SAIC Redefining Ingenuity™

Evolution: Incremental Improvements

The game is barely a year old, and has been used six times. Each training/demonstration event has given the game team opportunity to incrementally improve the scripting, content, attack/defense capability, and more. It is significant to note that the supporting team all support this capability in their spare time. There is no single game administrator or player coach that is dedicated.

Game Iteration	How did we evolve?
2016-Jul: Board of Directors	• Designed game for cyber novices • Converted attack/defense demo into a scripted, team-based activity • Introduced multiple social vectors
2016-Nov: Vendor Alliance Partners	• Enhanced content to appeal to technical audience
2017-Feb: AFCEA Cyber Symposium	• Ported environment to roadshow hardware
2017-Jun: GEOINT 2017 Symposium	• Tailored attack and defense to include IP/geospatial content
2017-Jul: Internal Corporate Staff	• Enhanced social media content • Implemented survey for metrics capture
2017-Aug: TechNet 2017	• Tailored for military support for allied government, critical infrastructure

Results: Surprising and Positive

And, the results have been surprisingly positive, given the relatively low level of investment made in the game environment. Below is shown value defined from each stakeholder's perspective:

Game Use Case	Stakeholder	Results
Education	Non-Technical Corporate Staff	• Increased awareness of spear-phishing, call center scams • Improved understanding of recruiters for cyber skills

SAIC Redefining Ingenuity™

Cyber Wargaming: Lessons Learned Influencing Security Stakeholders

Game Use Case	Stakeholder	Results
Education	Technical Community	• Sharpened offensive and defensive skills with hands-on, live access
Brand Awareness	Conference Attendees	• Senior-level customer has asked for gaming proposal paper • Have 40 military staff signups for upcoming training
Opportunity Generation	Targeted Customers	• Game enabled comments from senior-level customers on current gaps, best strategies for engaging
Alliance Strengthening	Partner Program	• Invitation by one partner to bring game to their hosted event

Where Next?

Given the success of the wargame so far, the team plans more improvements for the next year. Some of the items on our backlog include:

- More efficient roadshow equipment, better system performance, support for more "seats"
- More targets to support Man in the Middle (MitM), Spear Phishing and Border Gateway Protocol (BGP) attacks.
- More Networks and assets to mimic quasi-integrated government/industrial targets
- Internet of Things (IoT) assets for both attack and defense
- Strengthening of Corporate Alliance Partner Content
- Integration with company Independent Research and Development (IR&D) capabilities for internet simulation, OSINT, Scenario Automation

About SAIC

SAIC® is a premier technology integrator providing full life cycle services and solutions in the technical, engineering, intelligence, and enterprise information technology markets. SAIC is Redefining Ingenuity through its deep customer and domain knowledge to enable the delivery of systems engineering and integration offerings for large, complex projects. SAIC's approximately 15,000 employees are driven by integrity and mission focus to serve customers in the U.S. federal government. Headquartered in McLean, Virginia, SAIC has annual revenues of approximately $4.5 billion. For more information, visit saic.com.

Author: Jason Nichols

Lab Director, iSpace Innovation Lab

SAIC Office of Technology

Jason.A.Nichols@SAIC.com

SAIC
Redefining Ingenuity™