Corporate Cybersecurity: A Serious Game
Introduction

The heavy cost of cyber crime and its exponential increase from year to year are a source of grave and costly concern to the corporate world.

Not only is the frequency of cyber attacks getting more and more alarming every year, the attacks themselves are scaling new heights of sophistication and stealth.

A combination of these two factors is putting businesses at a serious disadvantage. As they are finding it more and more difficult to respond quickly to these security breaches. Research indicates that in 2012 it took a business 24 to 40 days to identify an attack and completely resolve it. Each cleanup is said to have cost $592,000. This cleanup cost shows a 42% increase from the average reported 2011 cleanup cost of $416,000.

Cyber crime cost U.S. business $8.9 million in 2012. The cost showed an increase of 6% from 2011 and 38% from 2010. (2012 Cost of Cyber Crime Study)
Cybersecurity Landscape in 2013
Top Security Threats to Businesses in 2013

Social Media
Given the growing influence of social media, especially in online revenue oriented activities, it will be the biggest source of cyber crime in the year to come. In 2013, social media sites will be the most targetted sites by cyber criminals looking for all kinds of personal, financial, and social security data. Social networks like Facebook and LinkedIn can be misused are most for manipulating people into performing actions or divulging confidential information.

BOYD
The increasing trend of BYOD at work places is the trojan horse of the virtual world. All kinds of smart devices, including phones, are making their way into the workplace. With these devices having access to an organisation’s networks, each one is virtually acting as a possible gateway for attackers. In view of the physical proximity of these devices to secured data sources, Near Field Communication capabilities will be used in 2013 for committing and cyber crimies.

Cloud Computing:
The increasing trend of cloud computing, wherein more companies put more information in public cloud services is a big risk. These services can represent a single point of failure for the enterprise. For businesses, this means that security must continue to be an important part of the conversation they have with cloud providers, and the needs of the business should be made clear.

HTML5
HTML5’s cross-platform support and integration of various technologies renders it vulnerable to attack. The newness of it means that attackers will be lying in wait for developers to make mistakes as they use it, and take advantage of the mistakes.
Types of Attacks in 2013

**APTs**
- Advanced Persistent Threat (APT) hacking attacks that use illegal means to get continuing and persistent access exfiltration of data.
- These high end attacks breach the organisational walls.
- The newer versions of APTs are not only difficult to detect but also challenging to prevent with the help of standard practices. Hence they need constantly innovating security systems.

**Ransomware**
- Ransomware is a type of malware. It is used for extortion. The attacker distributes malware that either encrypts the contents of a system or locks it. The attacker then demands money from the victim in exchange for releasing the data and/or unlocking the system.
- There is no guarantee that the attacker will release data or unlock the system once the payment is made. The integrity of the data remains a concern if access is restored. It is expected that 2013 will see such type of malware and delivery mechanisms become more sophisticated.

**Hactivism**
- Attacks carried out as cyber protests for politically or socially motivated purposes, or “just because they can” have increased, and are expected to continue in 2013. Common strategies used by hactivist groups include denial of service attacks and web-based attacks, such as SQL Injections.
- Once a system is compromised, the attacker will harvest data, such as user credentials, to gain access to additional data, emails, credentials, credit card data and other sensitive information.

**Spear Phishing Attacks**
- Spear phishing is a deceptive communication, seeking to obtain unauthorized access to personal or sensitive data. It includes e-mail, text or tweet, targeting a specific individual. Spear phishing attempts are usually motivated by financial gain, trade secrets or sensitive information.
What Options do Businesses Have?
How can businesses do to lower their cyber crime-related costs?

In the United States, businesses with the lowest relative cyber crime costs tend to have good information security governance program, use some type of security intelligence and include training and education on cybersecurity for their employees. Cutting edge cybersecurity training, especially simulations and games, is slated to play the biggest and most effective role in stalling cyber crimes and minimizing its costs to businesses.

Training to Change the Game

The strongest cyber security systems cannot provide effective protection against cyber attacks because 70% of cyber security breaches occur due to the human factor or the ‘insider threat’. Employees represent the key to reducing the human error factor and improving general organizational cyber security. More than half of the reported breaches are caused by unintentional mistakes made by the employees.

This is leading to a growing consensus – in government and in the private sector - that more training and education are needed as these lead to more
responsible behavior.
Visionary companies are moving from a reactive, defensive mode to a more pro-active approach, linking information security back to business strategy and putting in place mechanisms to ensure it.

TIS Cybersecurity Consulting

TIS Cybersecurity Consulting has evolved a needs evaluation and umbrella training curriculum to meet the challenge faced by businesses due to the cybersecurity issues.

The consulting phase is an individualized, fact-gathering process that maps the systems, needs and vulnerabilities of an organization. We then map the training requirements of the organization to the various components of our umbrella-training curriculum to develop a customized training solution for the client’s needs.

Our consultancy process includes:
• Gathering analytics on an organization’s weaknesses
• Identifying vulnerabilities that can be addressed through training
• Identifying a training curriculum for the organization
• Targeted training to attack the weaknesses
• Providing immediate feedback
• Reinforcing with short apps-based training nuggets
• Reassessing and retraining the employees that need it the most

TIS Cybersecurity Training Curriculum

A comprehensive cybersecurity-training program in an organization needs to be multi-tiered and nuanced to be effective. It needs to take into account the types of users, their skill levels, work profiles and roles and the security and IT infrastructure of the company. Our cybersecurity curriculum for businesses combines, employee awareness, compliance, specialist skills to combat threat and creation and implementation of policy.

The Training Matrix
The four categories mentioned above are addressed through innovative and engaging online solutions that address the underlying organizational objectives in a fun and engaging manner. Games and Simulations remain the mainstay of our training curriculum.

**Types of Solutions**

Our cybersecurity training curriculum leverages games and simulations to improve the cybersecurity profile of a business and move it away from a punitive and “check the box” mentality that unfortunately seems to inform most cybersecurity training initiatives at present. Traditional training has its limitations. When it comes to cyber security training these limitations become more pronounced.

The varied user base, motivation levels of users but above all the dynamic and rapidly changing nature of the threats themselves demand an innovative and hands on approach to training.

The pedagogy and design of our solutions delivers fun and engaging learning that allows the learner to be in control.

Our cybersecurity curriculum includes the following:

- Serious Games
- Simulations
- Gamification
- Virtual Labs
- Apps
- Tournaments

**Serious Games & Simulations**

Games are powerful tools – of fun and learning. Cybersecurity training lends itself to this concept due to the nature of the subject matter. The average person will ignore or forget content from emails with security warnings or company lectures when it comes time to actually applying that knowledge.

Serious games ensure a hands-on, non-scripted experience inside a realistic environment that fosters situational awareness, complex decision-making and attention to details. Learner motivation and therefore the effectiveness of any training program soar if one is able to immerse learners in a game in which they play a critical role. Games are part of our curriculum for awareness, compliance and specialized training.
Example: CyberCity
The game is modeled on SimCity™. It spans a virtual world that mimics configurable firewalls, VPNs, link encryptors and access control mechanisms within a town. The learner has to identify and resolve attacks that include corrupt insiders, viruses, Trojan horses, denial of service attacks, trap doors, and exploitation of vulnerable systems. Scenarios range from phishing attacks to ransomeware and APTs.

The players set up, operate and defend networks and like SimCity are able to see the impact of their actions. They are in charge of workstations, servers, operating systems, applications, and network devices, firewalls etc. The constraints they face mimic real life concerns in any organization like budgets, productivity and security.

The game progresses to more complex levels as users defend and protect critical security infrastructure where the stakes are increasingly higher.

Simulations
Simulations are the most effective training format for cybersecurity training. The USP of a simulation is that it presents scenarios that challenge learners at just the right level and then pushes them to the kind of expertise they need to attain.

Simulations are part of our curriculum for compliance, specialized and policy training.

Example: CyberArrest
CyberArrest is a concept we have developed that simulates an office environment. Players can play a number of roles. They can select an avatar at the start of the simulation. Depending on the role they have selected they go about their business in the office environment. It is within these daily, routine activities that threats lurk and they are required to spot them. As they manage and observe employees they may discover an insider who could pose a problem to the organization. The Sim tests the awareness levels of the employees and then allows them to select ways to resolve the issues they find.

Challenges are embedded into the learning architecture of the Sim.

Gamification
Gamification is an excellent tool for cybersecurity awareness training as engaging security awareness training needs to be done in a non-threatening
and non-challenging environment so that end-users feel less threatened to ask questions, have open dialogue and increase their knowledge of how to protect online identities, as well as corporate information. Gamification is the use of mechanics of gaming to nongame activities to change people's behavior. It is an important and powerful new strategy for influencing and motivating groups of people.

Micro-games with a cyber security awareness twist designed around key security threats like Social engineering, password protection, phishing, malware etc., are an effective way to demystify cybersecurity and ensure performance improvements in responding to attacks and thereby reduce an organizations susceptibility to attack.

**Example: Phishing Game**
This is a unique game format that delivers dummy threats to employees in an organization and thus tests their awareness levels. Based on the response of the employee it delivers focused and customized learning to the concerned employee. It helps in raising employee awareness and “buy-in” on information security best practices.

The user differentiates between the ‘good links’ (learning nuggets for training) and rejects the bad ones (spam links). The ‘good links’ and less bad ones the user clicks the more points they get. The players performance improvements in responding to phishing attacks will improve.

**Virtual Labs**

The application of virtualization technologies to the study of computer security has had the most significant impact through the development of specialized laboratories utilizing workstation or server based virtualization. Virtual labs support cybersecurity research and education, training, and awareness. The labs are characterized by innovation and variety.

Virtual Labs are part of our curriculum for specialized training.

**Example: CyberZone**
CyberZone offers a system for hands-on cybersecurity training in a remote virtual lab environment on the web. The platform provides individual learning environments for each student. The LMS enables online classes where an instructor can set up assignments and projects for each student. The students can upload theoretical papers and assignments on the LMS and conduct practical exercises in the virtual laboratory.
APPs

Apps are addictive and ubiquitous. The ‘engagement quotient’ of Apps is very high. Almost every smartphone user is uses some or the other app in their day-to-day life. They ensure appealing interactivity, heightened usability and user engagement. In the field of education and training too Apps are making a significant impact. An App for cybersecurity training will use these features to its advantage.

Apps are part of each component in our cybersecurity curriculum. They provide performance support and ongoing refresher learning support.

Example: CyberCecure App
The App combines first person shooter mechanics. Learners are given different scenarios. Learners can choose and strategically place firewalls, encryption techniques and anti virus systems. The more a learner plays, the more they are rewarded.

TIS Case Study
UMUC: Master of Science in Cybersecurity

“... At the University of Maryland University College, we engaged TIS to assist us with the development of media and learning objects in support of a very large and strategically important online program in cybersecurity. We have been very pleased with TIS’s work on this project. The synergies between their team and our faculty and staff have been excellent. Their technical expertise and ability to scale are impressive. They have delivered high-end course development of which we are very proud, and they have accomplished this on time and within budget."

Greg von Lehmen, Ph.D
Provost
UMUC
Day in the Life: A Dynamic Cybersecurity Simulation Solution

Test Drive your Workday Today

The Client

Founded in 1947, University of Maryland University College (UMUC) is one of 11 accredited, degree-granting institutions in the University System of Maryland (USM). Offering a broad range of cutting-edge classes, UMUC has earned a global reputation for excellence as a comprehensive virtual university and for focusing on the unique educational and professional development needs of adult students. Headquartered in Adelphi, Maryland, UMUC has classroom locations in the Washington, D.C., Europe, and Asia, and provides online classes to students worldwide.

Training Need

The Day in the Life module was developed as part of a larger training program for UMUC.

UMUC offers Bachelor’s and Master’s degrees in Cybersecurity, through a course that is completely online. Students who are currently working full-time can thus take this course while keeping their jobs, enabling them to apply for cybersecurity job roles.

UMUC felt that while the standard web-based training approach was of merit, learners also needed to relate their cybersecurity learning to the real world. With this in mind, UMUC desired a simulation-based approach that learners could play towards the end of the course.

Figure 1: Welcome: The learner is introduced to the simulation.
Learning Gaps/Problems
To identify any shortcomings and gaps in learning, the TIS team engaged in a discussion with the stakeholders at UMUC to identify learning gaps of students.

The issues that came across were:
• Inability to map cybersecurity issues learnt online to actual issues in the real-life job
• Managing people is part of good cybersecurity; handling them correctly is difficult to learn from web-based training alone
• Lack of a ‘fun’ aspect to learning cybersecurity; learners needed a break from a rigorous online course schedule

Figure 2: Colleague Profiles: The learner is introduced to the people that they’ll work with.

Design Thinking
TIS professionals then used these findings to drive the design thinking, with the following objectives being used to design the solution:

1. **Ground** the students in the day-to-day responsibilities of a cybersecurity professional.
2. **Test** their ability to make decisions related to cybersecurity.
3. **Engage** them in the solution for better learning by introducing elements of prioritization, time pressure, and immediate real-life feedback through e-mails, phone calls, and face-to-face conversations.
4. **Apprise** them of the consequences of botched decisions through the use of appropriately delivered feedback
Figure 3: A Scenario-related Call: Learners are asked to navigate scenarios based on e-mails, calls, or face-to-face conversations

Appendix
http://www.forbes.com
2012 Cost of Cyber Crime Study