# The Strategic Cybersecurity Threat Analysis Framework

*Know Your Enemy, to Defeat Your Enemy*

**Michele Myauo**
George Washing University PhD Candidate
Microsoft Director of Cybersecurity
michelem@microsoft.com, 703-673-7607

# Agenda

- **Approach Overview**
- **Know Your Enemy**
  - The Global Cyber Threat
  - What is a Targeted Attack?
  - Anatomy of a Cyber Attack
    - Dynamics of a Cyber Attack
    - Phishing Email Decomposed
    - Pass the Hash Technique
- **Defeat Your Enemy**
  - NIST Cybersecurity Framework
  - Security Engineering
  - Spotting a Phishing Email
  - Mitigating Pass the Hash
- **References**

**The following presentation reflects research conducted in conjunction with my dissertation work at the George Washington University**

# Approach Overview

***Either you're under attack and you know it ….Or you're under attack and you don't know it yet***

- Cyber attackers are successfully gaining access to corporate and government networks worldwide, threatening the global economy and security of the Nation
- Current Cybersecurity mitigation strategies focus on technical security *standards compliance* and *vulnerability mitigations* which are not sufficient in protecting organizational assets against live, advanced, and persistent threat actors
- Live attackers respond to changes in tactics and techniques in real-time, focusing on exploiting the weakest link in the enterprise architecture
- Cyber attacks exploit people, process, and technology to steal high value organizational data; therefore, organizations must address data security as it relates to people and their behavior, organizational processes, and technologies to mitigate cyber attacks

# Know Your Enemy

**Who** **Why** **What** **Where** **How** **When**


- ***Who*** would want to attack your organization?
- ***Why*** would an adversary want to attack your organization?
- ***What*** data and information would a cyber attacker want?
- ***Where*** is your organization most vulnerable to attack
- ***How*** will the attacker launch the attack against your organization?
- ***When*** is the attacker likely to strike?

# Know Your Enemy: The Global Cyber Threat

**Many taxonomies exist, but there is no internationally agreed upon taxonomy of cyber adversaries. Three common adversary types are identified below:**

## Insider Threat

- **Saudi Aramco** – An Insider "unleashed a computer virus to initiate what is regarded as among the most destructive acts of computer sabotage on a company to date." Erasing "three-quarters of Aramco's corporate PCs — documents, spreadsheets, e-mails, files — replacing all of it with an image of a burning American flag" (New York Times, 2012)


## Hactivist

- **The New York Times** – A hactivist group that supports Syrian President Bashar al-Assad, claimed responsibility for a cyber attack that took The New York Times website down for several hours in August 2013. The attackers rerouted internet traffic directed at the Times to other websites (CNN Money, 2013)

## Cybercriminals

- **US Department of Energy** – Cybercriminals stole personal identifiable information (PII) from approximately 53,000 federal employees to include dependents and contractors names, Social Security numbers, and date(s) of birth (DOE, 2013)

# Know Your Enemy: What is a Targeted Attack?

## Targeted Attack Defined *(Sood et.al 2013)*

- **Targeted Attack** – A Cyberattack directed toward a specific entity (individual, group, business, government body). The more sophisticated attacks leverage a combination of tools, social engineering tricks and tactics
- **Advanced Persistent Threats** - Subset of targeted attacks that evolves continuously through time, not necessarily more advanced than other attacks, just more patient

## The Three Phases of Targeted Attack *(Sood et.al 2013)*

1. **Intelligence Gathering** – Attacker gathers information on the target of the attack from publically available sources, also know as open source intelligence (OSINT)
2. **Develop Attack Model** – Attacker analyzes information gathered and reconstructs the target environment to plan the attack. Attackers identify most vulnerable employees and networks and take the path of least resistance
3. **Launch the Attack** – Attacker launches the attack against the target. Attack patterns very depending on information gathered and environment

# Know Your Enemy: Anatomy of a Cyber Attack

**Figure 1: Targeted Cyber attack Overview *(Sood et.al 2013)***

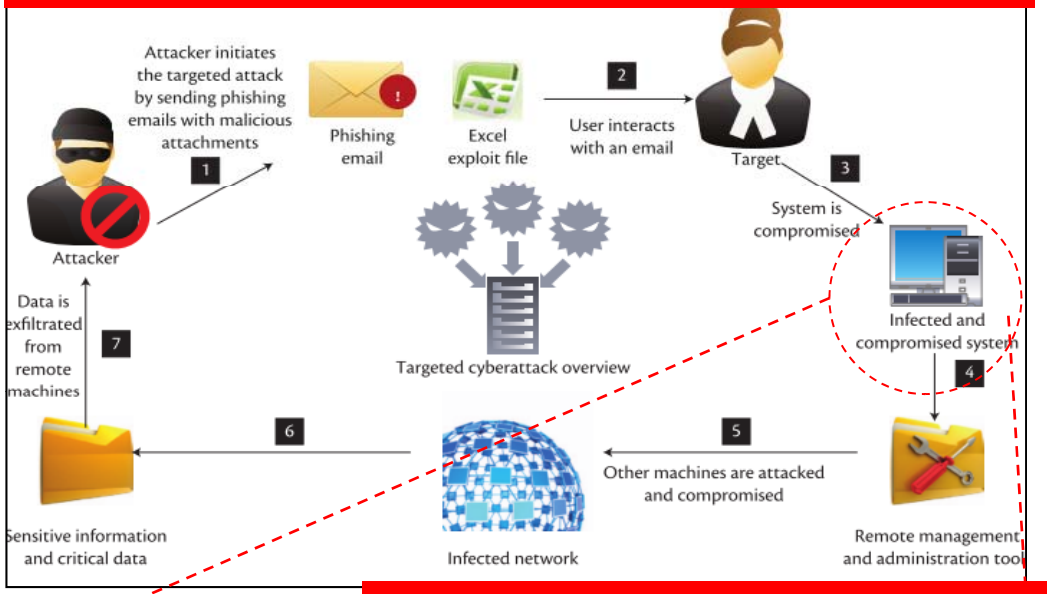
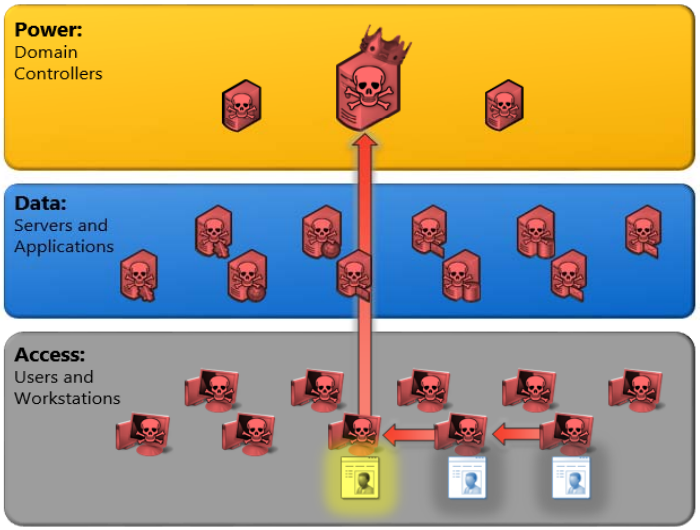



**Figure 2: Sample Phishing Email *(Myauo, 2013)***


**Figure 3: Pass the Hash Technique: *(Jungles & Simos, 2013)***




- In a cyber attack, the attacker targets people, processes & technologies
- "Pass the Hash" has been identified as one of the top cyber threats by government, academia, and industry
- This attack will be outlined in detail in the following slides

# Know Your Enemy: Dynamics of a Cyber Attack

**Figure 1: Targeted Cyber attack Overview**
***(Sood et.al 2013)***

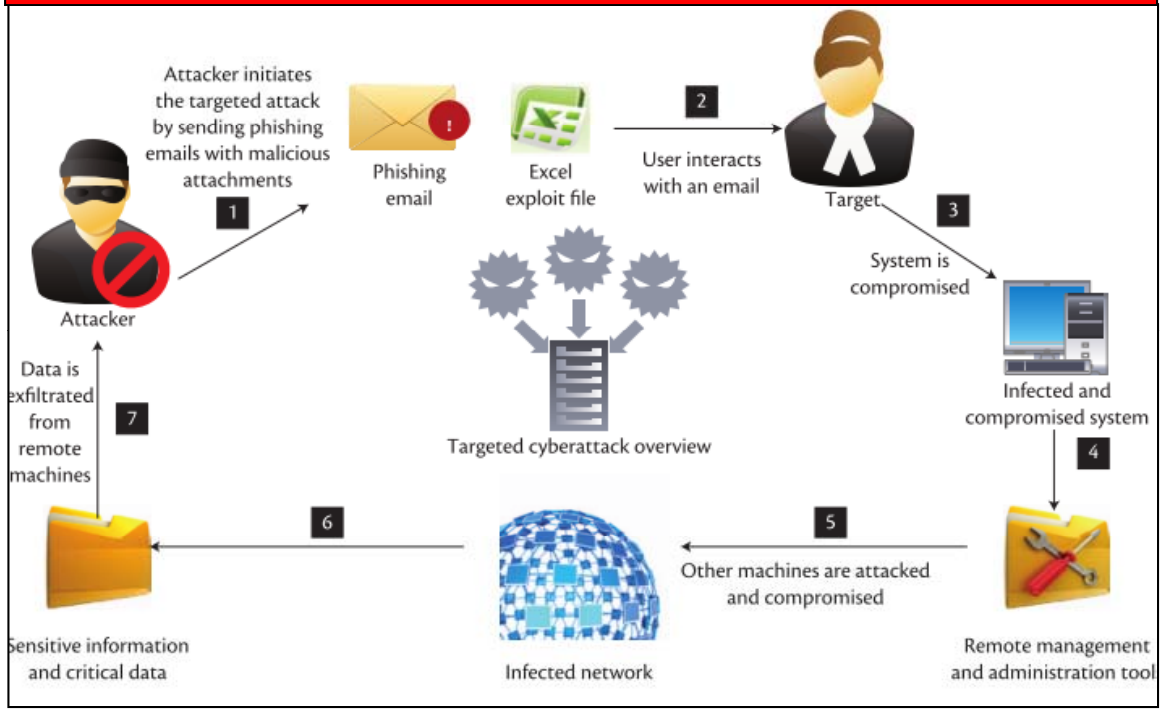



**Figure 1 provides an overview of a targeted persistent threat**

- Specifically, this attack shows a phishing email that is carrying an exploited code in the attachment (such as .DOC, .PDF, .XLS)

**In a targeted attack, an organization's people, processes, and technologies are targeted**

- Security standards compliance and vulnerability mitigations are not sufficient in protecting organizational assets against live, advanced, and persistent attackers
- Live attackers respond to changes in tactics and techniques in real-time, focusing on exploiting the weakest link in the enterprise architecture

# Know Your Enemy: Phishing Email Decomposed

**Figure 2: Sample Phishing Email**
*(Myauo, 2013)*


From: American Express [mailto:CCSG2@email2.americanexpress.com]
Sent: Thursday, August 08, 2013 5:58 AM
Subject: Card Service Alert: IMPORTANT about your Card Account.

IMPORTANT Notice for your CardMember Service

Dear Valued CardMember,

As part of American Express Online commitment to provide you with exceptional service, American Express Online is taking additional steps to ensure that your account data is secure.

We are sending you this e-mail as a security notification, to confirm to you the inability to accurately verify your account information due to an internal error within our server.

You are required to review your account information to prevent any future attention with your card online access.

To get started, we have sent you an attached HTML Web Page.

- See Attached for HTML Web Page
- Download and Save it to Desktop
- Go to Desktop to open the HTML Web Page
- Get Started by Filling your Information

Thank you for your continued Cardmembership.

Sincerely,

American Express Customer Care

Was this e-mail helpful? Please Click here to give us your feedback.

For your security:

Account Beginning: 37XX X

Your Credit Score Matters

Obtain your Complimentary Credit Score and Report today. Your credit impacts all areas of your financial life. Learn what is being reported about you and much more.

Learn More

1

2

## What is a Phishing Email?

- Email that tries to trick you into providing personal information or providing access to your computer network by impersonating a legitimate business

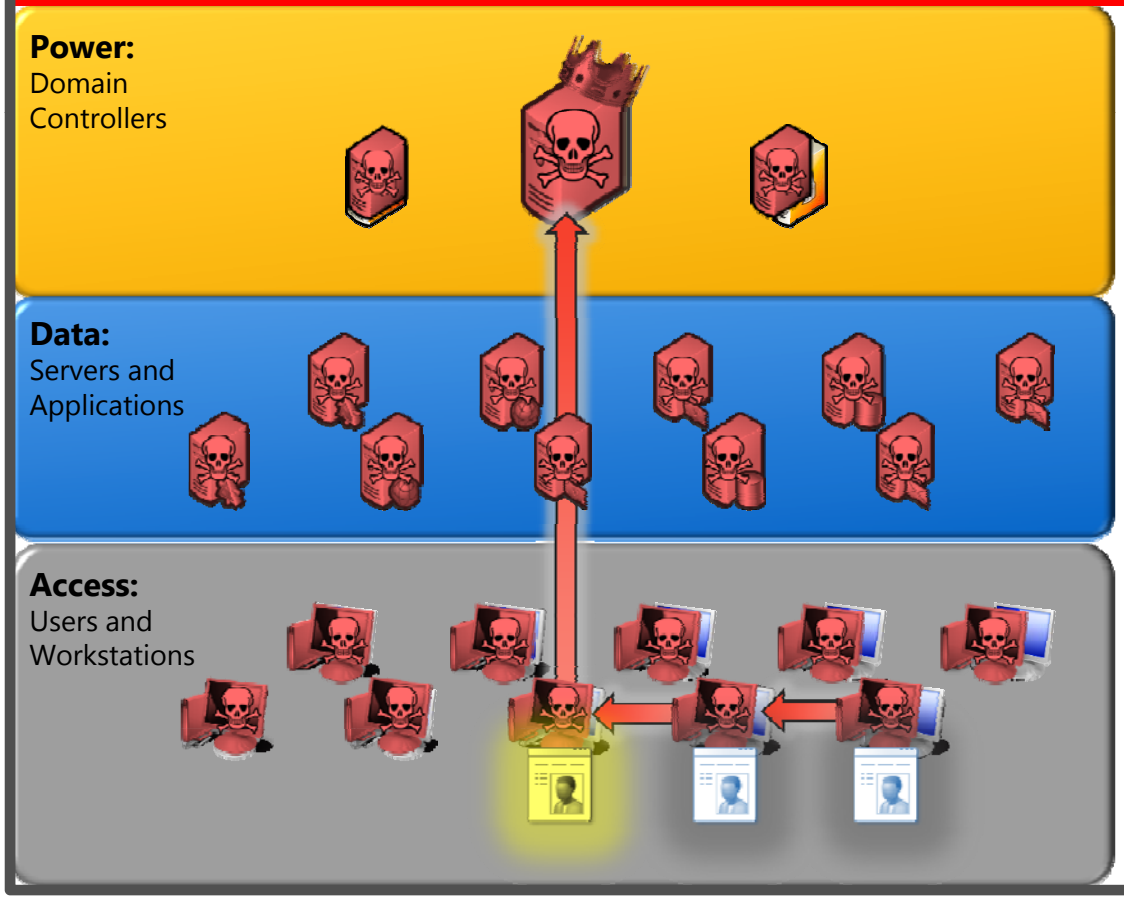
## Hints this may be a Phishing Email:

1. Says that you should download a HTML file, save to the desktop and open it
2. Uses the first portion of your card number as opposed to using the end. Amex, Discovery, Visa, MC, etc., all have specific prefixes...so everyone's Amex starts with 37
3. "Would AMEX send this?"; this email is excessively technical for the average user
4. If you copy the link that is hidden under the textual link, paste it in a notepad and verify the domain

# Know Your Enemy: Pass the Hash Technique

- The Pass the Hash attack scenario is identified in academia, government and industry literature as a common attack technique

**Figure 3: Pass the Hash Technique**
***(Jungles & Simos, 2013)***




1. Attacker targets workstations en masse
2. User running as local admin is compromised, attacker harvests credentials
3. Attacker uses credentials for lateral movement or privilege escalation
4. Attacker acquires domain admin credentials
5. Attacker starts exercising this full control of data and systems in the environment

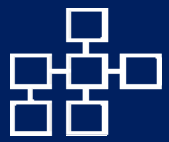
# Defeat Your Enemy

**Organizations must address security as it relates to people, process, and technology in order to keep high value organizational data safe**

**People**

- Determine who should have access to high value organizational data
- Educate employees on cybersecurity threats. This sounds simple but takes time, resources, and ongoing commitment by the organization For example: “Do employees know how to identify and report a phishing email?”, “Would employees recognize social engineering?”

**Process**



- Institute secure organizational processes. For example good credential hygiene
- Organizations should bake security into system design and can incorporate secure development practices in all phases of the systems engineering process, from envisioning through implementation and maintenance

**Technology**

- Architect your enterprise in a way that makes it technically difficult for attackers to infiltrate the environment
- Consider the appropriate access, location, method of storing organizational data either internal to the organization or external (e.g., Onsite, Cloud, Hybrid-Cloud)

# Defeat Your Enemy: NIST Cybersecurity Framework


**Under Executive Order 13636 "Improving Critical Infrastructure Cybersecurity," NIST is working with SMEs to develop a framework to reduce cyber risk to critical infrastructure**

**The NIST Cybersecurity Framework will focus on 5 key areas that include Know, Prevent, Detect, Respond, and Recover**

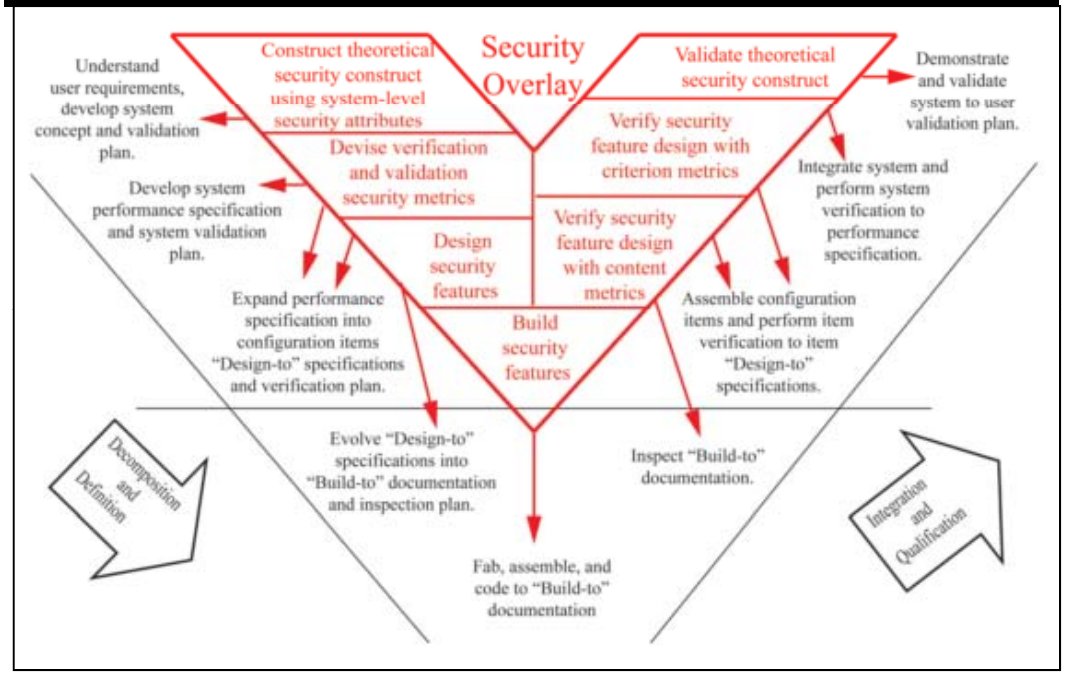
- These areas are currently being defined by NIST with involvement from the general public, industry, academia, and government

**Join the Discussion**

- The 5th Cybersecurity Framework Workshop will be held in Raleigh, NC on November 14-15, 2013
- Find out more and get the latest information at: http://www.nist.gov/itl/cyberframework.cfm

# Defeat Your Enemy: Security Engineering

**Figure 4: Security Metrics in the Vee Model**
*(Bayuk & Mostashari, 2013 )*




**The framework identifies where security principles should be integrated into the traditional Systems Engineering V**

- Begin by defining security critical to the system's mission
- Capture system level security requirements
- Develop security architecture metrics
- Validate that the system meets security needs
- Ensure personnel are properly trained

# Defeat Your Enemy: Spotting a Phishing Email

**What should I do if I receive a Phishing email to my corporate email?**

- Tailored phishing emails look like they know something about you, your organization, your role and goes to your corporate account
- The attacker knows the business you are in and the attacker knows what company they are sending the email to

**What should I do if I receive a Phishing email?**

- ✓ If you or people within your organization receive a phishing email addressed to a corporate account, let your company know as you may be under attack
- ✓ You may also report phishing to:
  - US Federal Trade Commission http://www.consumer.ftc.gov/articles/0003-phishing
  - USCERT http://www.us-cert.gov/report-phishing/



***When in Doubt, Don't Click***

# Defeat Your Enemy: Mitigating Pass the Hash

## What can your organization do to mitigate a Pass the Hash?

- Read the Microsoft “Mitigating Pass-the-Hash Attacks and other Credential Theft Techniques http://www.microsoft.com/en-us/download/details.aspx?id=36036

## Overview of Mitigations found in the whitepaper is provided below:

✓ **Mitigation 1 - Restrict and protect high privileged domain accounts**
- Reduces the risk of administrators from inadvertently exposing privileged credentials to higher risk computers
- Attacker cannot steal credentials for an account if the credentials are never used on the compromised computer

✓ **Mitigation 2 - Restrict and protect local accounts with administrative privileges**
- Restricts the ability of attackers to use local administrator accounts or their equivalents for lateral movement PtH attacks
- Attacker who successfully obtains local account credentials from a compromised computer will not be able to use those credentials to perform lateral movement on the organization's network

✓ **Mitigation 3 - Restrict inbound traffic using the Windows Firewall**
- Restricts the ability of attackers from initiating lateral movement from a compromised workstation by blocking inbound connections
- Attacker who successfully obtains any type of account credentials will not be able to connect to other workstations


Q
&
A

# References


- Bayuk, Jennifer, and Ali Mostashari. 2013. "Measuring Systems Security." Systems Engineering 16 (1): 1–14.
- CNN. "New York Times Hit with Malicious Attack." Accessed October 1, 2013. http://money.cnn.com/2013/08/27/technology/security/new-york-times-hacked/index.html
- DOE. "July 2013 Cyber Incident." Accessed September 1, 2013. http://www.doe.gov/cio/cyber-incident-information/july-2013-cyber-incident
- Microsoft. "Mitigating Pass-the-Hash Attacks and other Credential Theft Techniques." Accessed September 5, 2013. http://www.microsoft.com/enus/download/details.aspx?id=36036"
- Myauo, Michele. 2013. Phishing Email.
- New York Times. "In Cyberattack on Saudi, U.S. Sees Iran Firing Back." Accessed September 10, 2013. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0
- NIST. "Cybersecurity Framework." Accessed September 25, 2013. http://www.nist.gov/itl/cyberframework.cfm#
- Simos, Mark, and Patrick Jungles. 2013. "Pass the Hash and Other Credential Theft and Reuse: Mitigating the Risk of Lateral Movement and Privilege." Paper presented at Blackhat USA, Las Vegas, NV, July 27-August 1, 2013. Accessed September 20, 2013. https://www.blackhat.com/us-13/archives.html#Simos
- Sood, Aditya K., and Enbody, Richard J. 2013. "Targeted Cyberattacks□: A Superset of Advanced Persistent Threats." IEEE Security & Privacy (February): 54-61
- USCERT. "Report Phishing Sites." Accessed September 18, 2013. http://www.us-cert.gov/report-phishing/
- US Federal Trade Commission. "Phishing." Accessed September 18, 2013. http://www.consumer.ftc.gov/articles/0003-phishing