SECURING CYBERSPACE

Mr. Curtis W. Dukes
Director, Information Assurance
National Security Agency

THE STATE OF CYBER

CYBER THREATS ARE INCREASING IN SCALE AND IN SCOPE

Adversarial Objectives are Changing

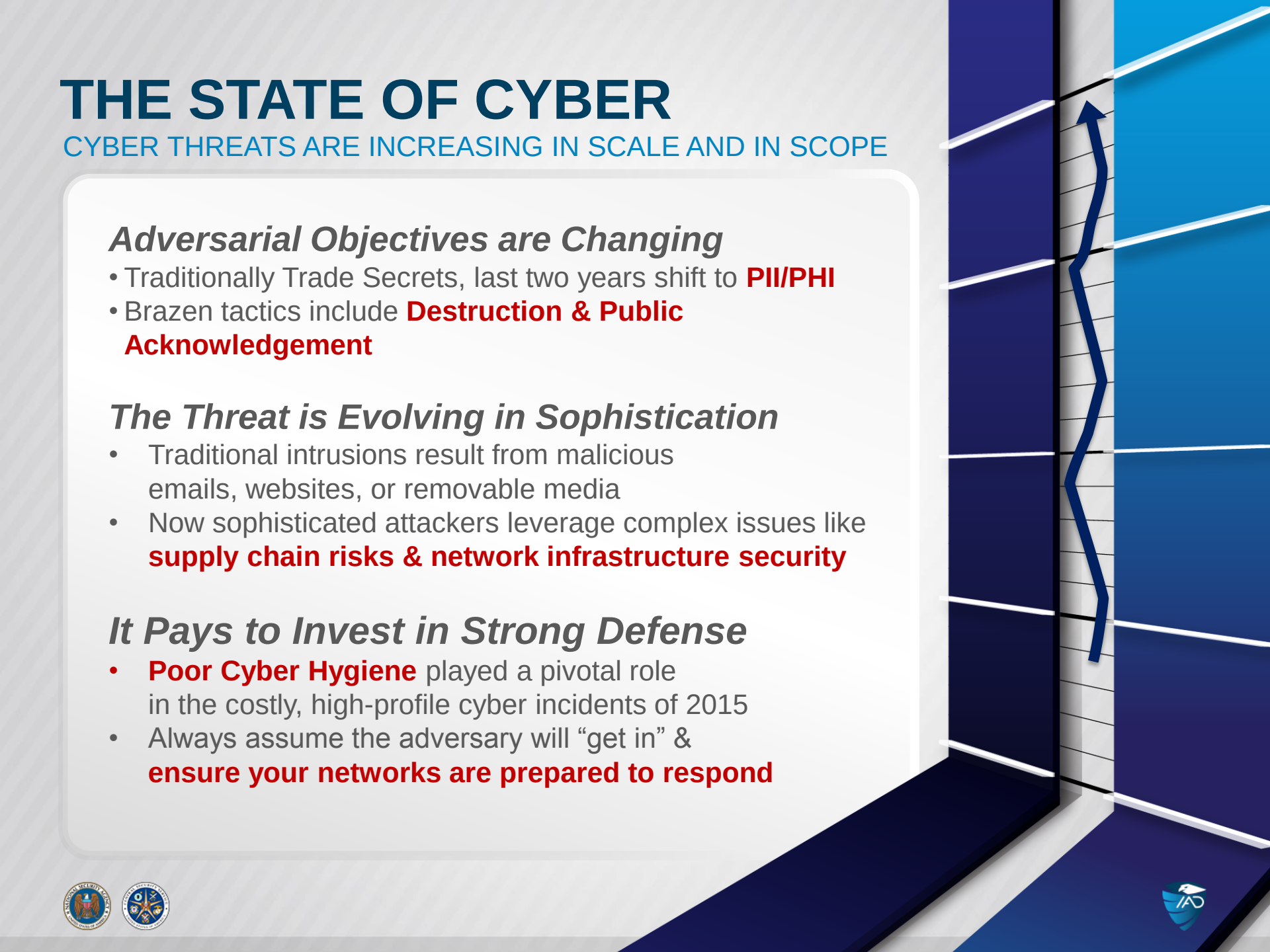
- Traditionally Trade Secrets, last two years shift to **PII/PHI**
- Brazen tactics include **Destruction & Public Acknowledgement**

The Threat is Evolving in Sophistication

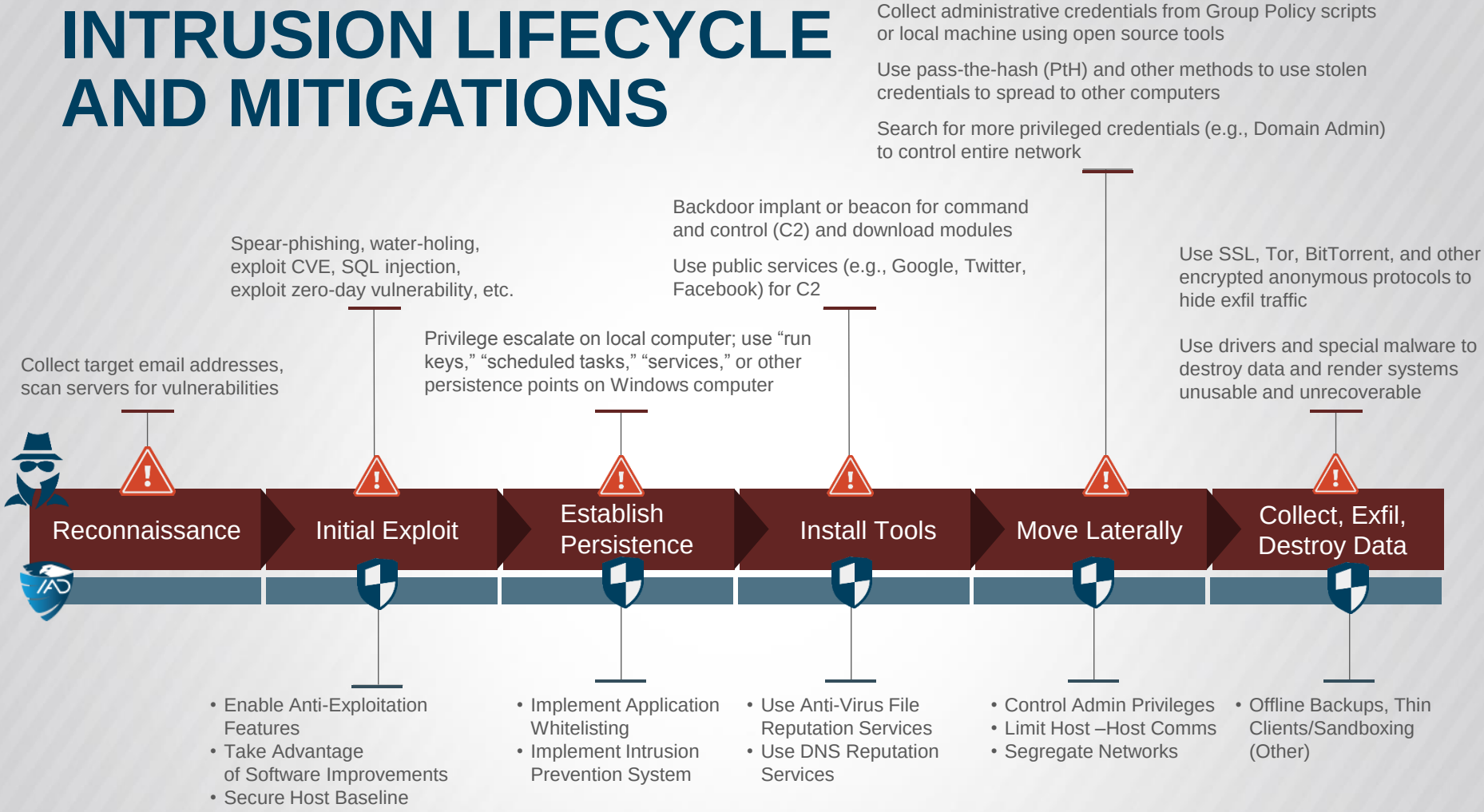
- Traditional intrusions result from malicious emails, websites, or removable media
- Now sophisticated attackers leverage complex issues like **supply chain risks & network infrastructure security**

It Pays to Invest in Strong Defense

- **Poor Cyber Hygiene** played a pivotal role in the costly, high-profile cyber incidents of 2015
- Always assume the adversary will “get in” & **ensure your networks are prepared to respond**



INTRUSION LIFECYCLE AND MITIGATIONS



Protections provided by the IAD Top Ten Mitigations & Host Mitigations Package

IAD TOP 10 MITIGATIONS AND HOST MITIGATIONS PACKAGES

IAD's Top 10 Information Assurance Mitigation Strategies

Fundamental aspects of network security involve protection and detection measures can be grouped in four mitig
goal areas. These four mitigation goal areas target critical steps in the intrusion life cycle — creating a technical la
defense approach that supports the ability to "fight through" a contested cyber environment:

- *Device Integrity* — maintaining and measuring device health/integrity. Devices often repr
attack surface area or the persistent living-space for the advanced persistent threat (APT).
- *Damage Containment* — when intrusions occur, limiting losses of information, system
mission capabilities.
- *Defense of Accounts* — protecting credentials from misuse and enabling trusted auth
access.
- *Secure and Available Transport* — maintaining the privacy and reliability of dat
communications.

These goal areas will support current and future cyber defense efforts, helping to set priorities, and
desired end-state of denying adversaries the ability to operate on our networks and impact our mis
be implemented now are listed below as IAD's Top Mitigations with goal areas indicated in the left
critical points in the attack life cycle, these mitigations are effective against entire classes of attack
unknown variants.

1. Application Whitelisting: Application Whitelisting is a proactive security technique
of approved programs to run, while all other programs and most malware are blocked fro
Application Whitelisting enables only the administrators, not the users, to decide which
run.

2. Control Administrative Privileges: Privilege escalation is the act of exploiting
configuration oversight in an operating system or software application to gain elevate
are restricted from normal users. Network owners should only grant Administrator
necessary and should take steps to ensure Administrator accounts are not exposed t
of increased risk. More robust protections can be achieved through the use of two-
administrators and other privileged accounts.

3. Limit Workstation-to-Workstation Communication: Pass-the-Hash (
allows an attacker to authenticate to a remote system by using the underlying h
having to know the actual password itself. Hackers generally use hashes from t
other machines, grabbing higher privileged credentials as they progress. A ra
to fully mitigate all the facets of Pass-the-Hash. One scalable and highly effec
workstation-to-workstation communication, thereby thwarting an attacker'
within the network.

The Information Assurance Miss

Host Mitigation Package (HMP)

Introduction

Our adversaries' command of modern technology and proficiency in exploiting vulnerabilities limits our ability to deploy computer network defensive capabilities in today's environment. The constant introduction of new applications and platforms – coupled with the exponential increase in computing power – creates an enormous challenge for system administrators to adequately defend against malicious activity taking place on the network. Detection of any new threat is often discovered only after data has been exfiltrated or other artifacts of an attack have been identified.

The normal response to any successful attack is to develop and deploy tools that will oppose that specific threat. However, that approach is reactionary in nature and does nothing to counter sophisticated adversaries that can easily overcome this type of signature-based response strategy by making simple modifications to their code. A proactive way forward that focuses on prevention rather than reaction is needed. As such, the Host Mitigations Package (HMP) is designed to aid organizations and system administrators in hardening their host systems.

Host Mitigations Package Overview

Most organizations tend to focus on securing the larger network. Devices such as firewalls, routers, and Intrusion Detection and Prevention systems get most of the attention from network administrators. Although securing the network is vital, hardening host systems is just as essential and deserves the same level of consideration. The Department of Defense (DoD) is working to address emerging host threats by implementing capabilities like the SANS Top 20 Security Controls. However, this effort is focused on a comprehensive program regarding host hardening.

HMP was constructed in order to corral the many disparate security controls into one package. The HMP supports the defense-in-depth strategy in which multiple layers of security controls are placed throughout a host. Any single layer of defense will most certainly contain gaps that could be exploited by an adversary. A series of different security defenses residing in a single host should be used to cover the gaps in other layers. The intent of HMP is to not only prevent security breaches, but also to buy an organization time to detect and respond to an attack. As such, an adversary that is not stopped cold will have to work harder and longer, thus reducing and mitigating the consequences of a breach. The HMP uses an efficient combination of operational tools designed to provide a layered defense against the most common and most effective techniques utilized by hostile actors.

This package was designed to implement existing commercial software to provide high gains at a low resource cost to increase overall system security. The HMP is modular and can be tailored to fit customer needs. The tools included in the package are: system configurations, freely available commercial software, or Government enterprise-licensed software, all of which are freely available for immediate download. Additional information for these tools is provided in the references below. System administrators should expect about two weeks to tune the software for optimal performance across their network. The HMP suite of tools works with the standard baseline of Microsoft® Windows XP®, Windows 7®, or Windows 8® operating systems[1].

The HMP includes the following capabilities:

1. Application Whitelisting
2. Anti-Exploitation Features
3. Anti-Virus Cloud Lookup
4. Host Intrusion Prevention System

Confidence in Cyberspace

December 2013
MIT-002FS-2013