Threat Assessment - Implementing Effective Security Controls

Aurelian BUZDUGAN
GCIH, GCFE, CEH, ENSA
aurelian.buzdugan@yahoo.com

Agenda

1. Threats / assets
2. Evolution of threats
3. Cyber attack scenario modelling
4. Recommendation on best practices

The Threat – Adversary – Bad Guy

Lone wolf?

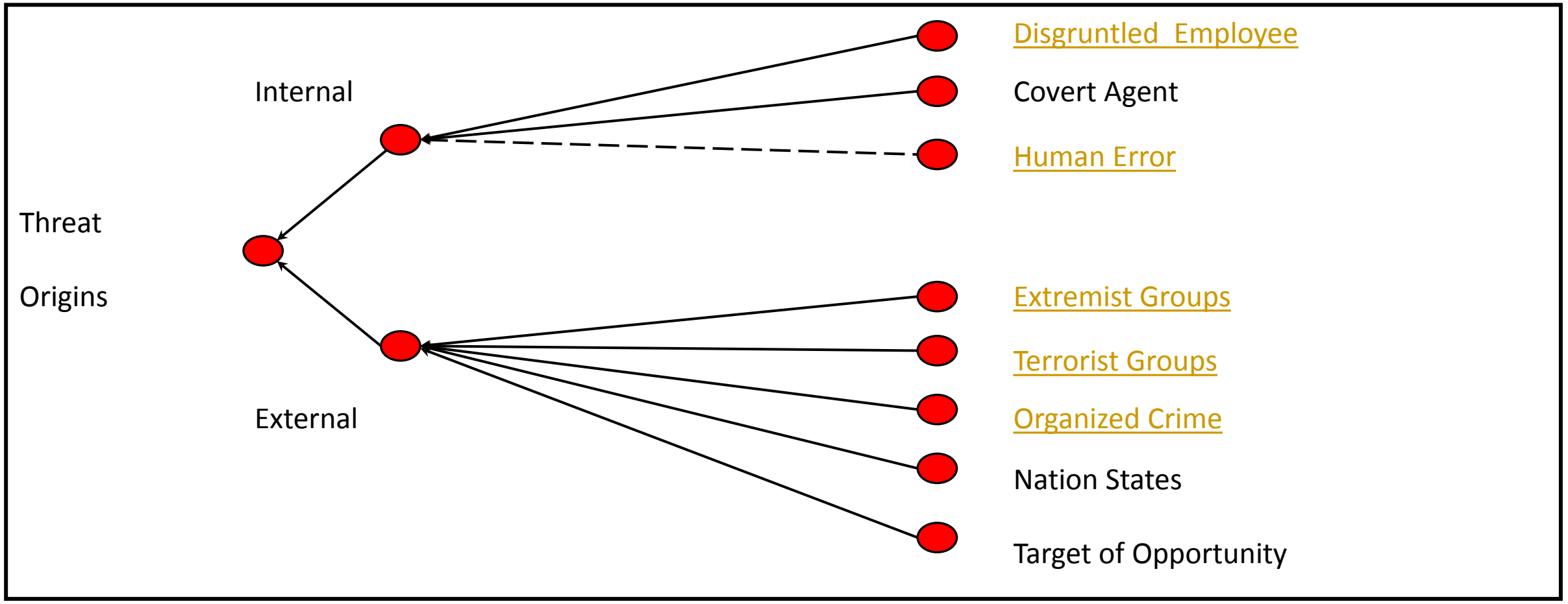
Trusted Employee?

Dedicated group?

Most people have a hard time understanding the threat and thinking like the adversary!

Source:IAEA

The Threat – Adversary – Bad Guy



Source:IAEA

All Targets are Vulnerable to something…

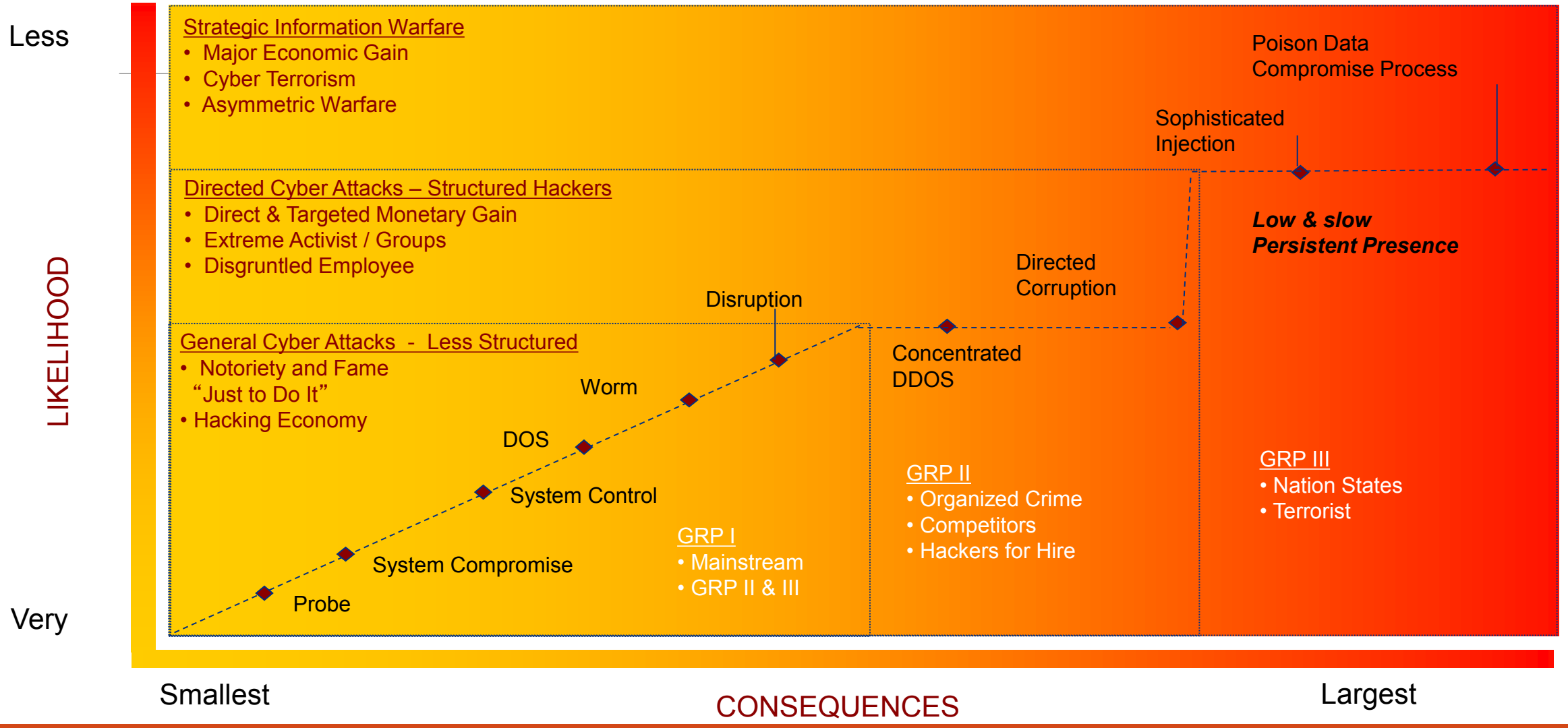
No target is completely free from all vulnerabilities including those resulting from:

- Failures in technology
- Errors in implementation
- A breach of trust by a human component

Generally, the more complex the system, the more likely it contains weakness.

Source:IAEA

Threat and Attack Characteristics



Proactive actions for the defense

Typical action after a breach – patch/adjust the security control

- Most of Security teams work like this

Goal of a SOC – close tickets in time to avoid SLA breaches

- Issues are tackled more from availability point of view

Proactive thinking for defenders is still uncommon

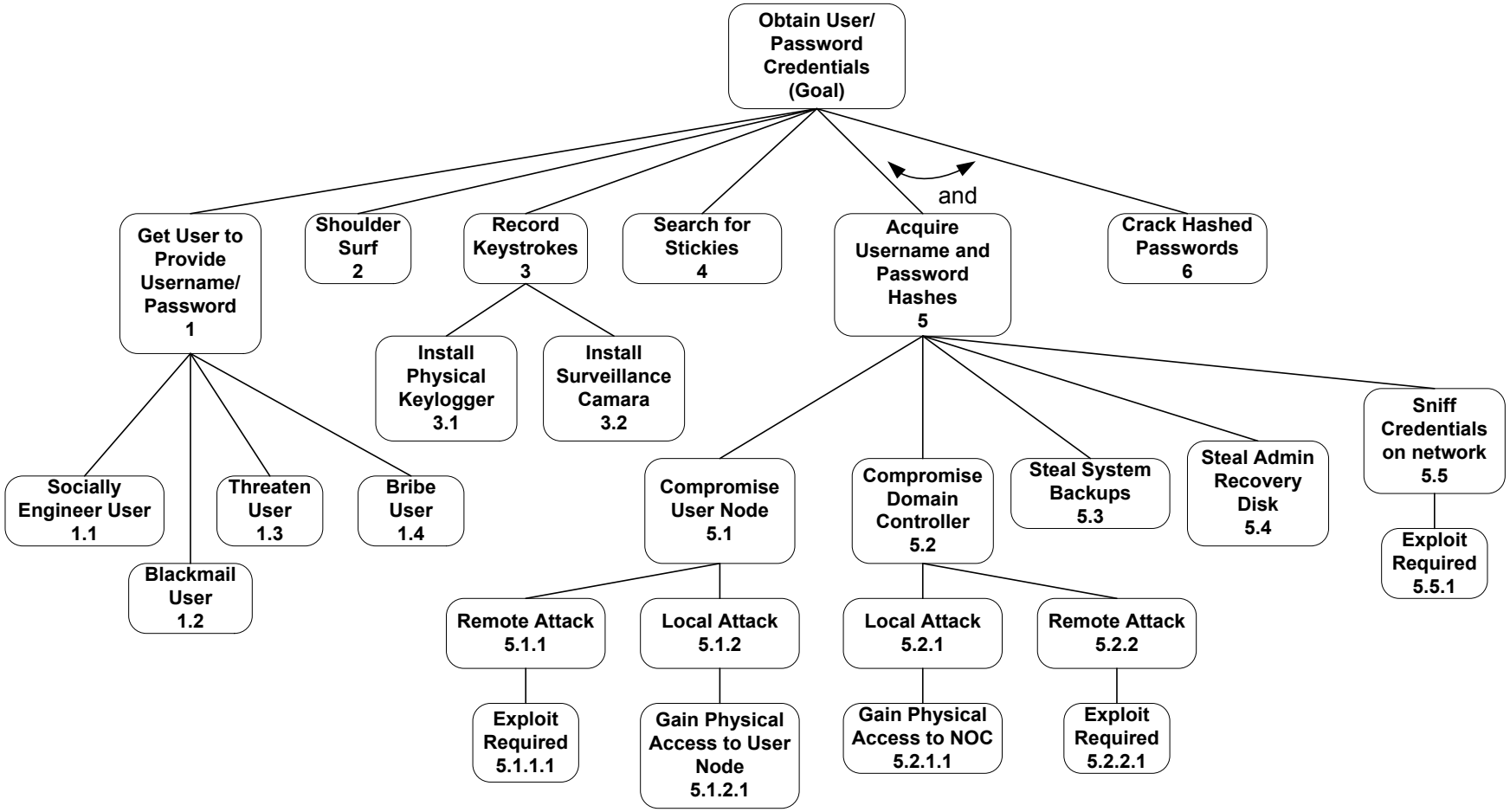
- Cyber campaign reports starting to reflect this new mindset
- Example: SANS Blackenergy
  - Documents what happened (as most of reports)
  - it describes as well **how could the attacker evolve** and **how should we evolve in defense**
- The novelty is changing the mindset – defense needs to be proactive
- Not just whack-a-mole game, where defense is built based on previous detected/published attacks, but also predicting what could the attacker come with

Cyber Attack Scenario Model

Goal of developing models of scenarios:

1. Identifying potential vectors or patterns for attack
2. Understanding where vulnerability exist
3. Understanding the effectiveness of countermeasures
4. Determining optimal use or placement of countermeasures
5. Focusing risk management efforts to address the most likely vectors of attack

Attack Tree example: Obtaining User Credentials



Source:IAEA

Secrets and Lies: Digital Security in a Networked World
Bruce Schneier, January 30, 2004 ISBN-10: 0471453803 | ISBN-13: 978-0471253112

Current situation

- Threat assessment is not an easy task
  - But we need to start somewhere
- Advanced threats are hard to detect & deter
  - But risks can be minimized

- Defense needs to be proactive in implementing security controls
  - Unfortunately many of the basic security features are still ignored…
    - Sysmon
    - EMET
    - Application whitelisting
    - Effective Patch & Vulnerability management
- Not all organizations have resources
  - But can at least implement the recommended good practices

System Monitor (Sysmon)

- You need: agent + configuration, WEF, WEC, SIEM
- No license costs
- Significantly increased visibility on endpoints
  - Threat detection
  - Forensic capabilities
- Monitoring tool – relative low risk for implementation (mind the GDPR!)
- Not a implement & forget tool –continuous effort required

Enhanced Mitigation Exploit Tool (EMET)

- Win 7 – standalone application, Win 10 (Creators update) – integrated part of Windows Defender
- Free exploit mitigation tool! (commercial products claim to be better, however not all organization have the resources)
- Highly customizable (feature/process/exception management)
- Events: false positive or actual incident?

Application Whitelisting (AppLocker)

- Feature available but needs to be enabled in Win 7/Win10
- Deployment needs to be well thought (requirements, deployment strategy)
  - Proper testing/piloting is mandatory
- Microsoft AppLocker gains popularity (commercial offerings also are improving)
- Significant security improvement
  - Only whitelisted executables can run
- And yes…it is not easy
  - can be run in audit mode at the beginning
  - should be a requirement for the migration to the next OS / AV
  - Leadership support & will to change

Summary

- The threats are out there…and becoming better every day
- Defensive controls need to be adapted to current threats and…anticipate the threats to evolve
- Scenario modeling can be effective for defenders in understanding their weak points and thinking like the adversary
- Good practices are published with a reason!