Cybersecurity in Plain English

A Practical Guide to Understanding Modern Cyber Risk

James P. Whitaker, CPCU

Smarts Publishing

*This sample includes selected chapters from **Cybersecurity in Plain English**, a practical guide to cyber threats and protections through an insurance lens. These chapters provide a preview of the book's plain-English approach to using insurance-focused examples to make cybersecurity concepts clear, relevant, and immediately useful in client conversations.*

Chapter 1 - MITRE ATT&CK

Most cyber conversations today reference "MITRE ATT&CK," but very few insurance professionals know what it actually is — or why it matters for underwriting, claims, and risk evaluation.

Where the name comes from:

MITRE (which is not an acronym, according to its founders) is the not-for-profit research organization that created the framework.

ATT&CK is an acronym for **Adversarial Tactics, Techniques & Common Knowledge** — a structured way of describing how attackers actually operate. MITRE began developing ATT&CK in 2013 as part of a research project to document real adversary behaviors observed in enterprise environments.

Here's the simple version.
MITRE ATT&CK is the industry's shared encyclopedia of attacker behavior.

It catalogs how attackers operate — the tactics they use, the techniques they rely on, and the patterns defenders should be able to detect.

Instead of vague descriptions like "malware activity" or "credential theft," ATT&CK gives teams a common language:

- T1055 — Process Injection
- T1003 — Credential Dumping
- T1021 — Lateral Movement

These codes show up in cyber applications, control assessments, SOC reports, and vendor claims. When a company says they "map to MITRE ATT&CK," they're saying:

"We understand the behaviors attackers use, and we've aligned our detection strategy to them."

Why this matters for insurance

ATT&CK helps reveal the gap between paper controls and actual detection capability. A company may claim coverage for a technique, but if the underlying logs aren't configured, the detection won't fire. That gap is where losses occur.

The takeaway

MITRE ATT&CK isn't a tool — it's a shared language. And understanding that language helps insurance professionals evaluate cyber maturity with far more clarity.

Chapter 3 - The Cyber Kill Chain

The attacker's playbook — and why understanding it changes everything

The Cyber Kill Chain is a 7 step model that explains how attackers plan, execute, and complete an attack.

It's the "script" behind:

- phishing
- ransomware
- BEC
- identity compromise
- lateral movement
- privilege escalation
- data theft

- cloud breaches

If you understand the Kill Chain, you understand how attacks actually unfold — and where defenders (and insurers) can break the chain.

The 7 Steps of the Cyber Kill Chain

1. Reconnaissance

Attackers gather information:

- employee names
- email formats
- vendors
- cloud apps
- exposed systems
- leaked credentials

This is where social engineering begins.

2. Weaponization

Attackers prepare their tools:

- phishing kits
- malware
- fake login pages
- malicious documents

- MFA fatigue scripts

This is the “loadout” phase.

3. Delivery

The attack is sent:

- phishing email
- SMS link
- malicious attachment
- MFA push spam
- poisoned website

This is where most people first notice something is wrong.

4. Exploitation

The victim takes an action:

- clicks a link
- enters credentials
- approves an MFA prompt
- opens a file

This is the human moment — the slip.

5. Installation

Attackers establish a foothold:

- install malware
- steal tokens
- create persistence
- enroll their own MFA device

This is where the attacker becomes “sticky.”

6. Command & Control (C2)

Attackers connect back to their systems:

- remote access
- beaconing
- control channels

This is how they coordinate the rest of the attack.

7. Actions on Objectives

The attacker completes their mission:

- ransomware
- data theft
- wire fraud
- privilege escalation
- lateral movement
- cloud takeover

This is the part that becomes the claim.

Why the Kill Chain Matters for Insurance:

Every major cyber claim maps cleanly to the Kill Chain.

- Social engineering → Steps 1–3
- MFA fatigue → Step 4
- IdP compromise → Steps 5–7
- Privilege escalation → Step 7
- Lateral movement → Step 7
- Ransomware → Step 7
- BEC → Steps 4–7

And here's the underwriting nuance:

The earlier you break the Kill Chain, the cheaper the claim.

The later you break it, the more catastrophic the loss.

Controls that matter:

- phishing resistant MFA
- conditional access
- identity analytics
- EDR/XDR
- network segmentation
- privileged access management (PAM)
- Zero Trust
- vendor payment controls
- continuous monitoring

The Kill Chain is the map.
Controls are the roadblocks

Real-World Incident
A manufacturing company suffered a ransomware attack.
When investigators mapped the incident to the Kill Chain, it looked like this:

1. **Recon** — attacker scraped LinkedIn for employee names
2. **Weaponization** — created a fake Microsoft login page
3. **Delivery** — sent a spear-phishing email
4. **Exploitation** — employee entered credentials
5. **Installation** — attacker enrolled their own MFA device
6. **C2** — attacker connected through a remote access tool
7. **Actions** — deployed ransomware across 2,000 endpoints

The entire attack took **less than 48 hours**.

The claim exceeded **$14 million**.

Understanding the Kill Chain isn't academic.
It's practical.

Film Parallel (U.S.)

In *Ocean's Eleven*, the heist follows a precise sequence — reconnaissance, preparation, infiltration, execution. The Cyber Kill Chain is the real-world version of that structure.

Novel / Non-Fiction Parallel

In *The Cuckoo's Egg*, Clifford Stoll tracks an attacker through each stage of the Kill Chain before the model even existed.
And in *Future Crimes*, Marc Goodman explains why understanding attacker workflows is the key to stopping them.

Both reinforce the same truth:
Cybersecurity isn't random — it's patterned.

Vocabulary Reinforcement

- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control (C2)
- Actions on Objectives

About the Author

James Whitaker, CPCU, is the publisher of Smarts Publishing and the author of the Plain-English Insurance Series. He has spent more than three decades helping insurance professionals understand complex topics through clear, accessible writing. His books, newsletters, and training materials are used by agencies, brokers, and carriers across the country.

With AI in Plain English, Whitaker continues his mission of making emerging insurance concepts understandable for everyday professionals. His work focuses on clarity, practicality, and real-world application — helping readers build confidence in a rapidly changing industry.

About Smarts Publishing and the Plain-English Insurance Series

Smarts Publishing creates clear, practical insurance education for agents, brokers, underwriters, and other insurance professionals. The Plain-English Insurance Series is designed to make complex topics easy to understand and easy to communicate to clients. Each book focuses on clarity, relevance, and real-world application — helping professionals build confidence

and competence in today's rapidly changing insurance environment.

Other Books in the Plain-English Insurance Series

• *Cybersecurity in Plain English* • *Cyber Liability in Plain English* • *Property & Casualty Insurance in Plain English* • *Insurance Fundamentals in Plain English*