# Probability in Cyber Risk Assessment: Holy Grail or Red Herring

## *A Community Discussion*

JOSHUA COLE, CISM


WELCOME

# This discussion is interactive

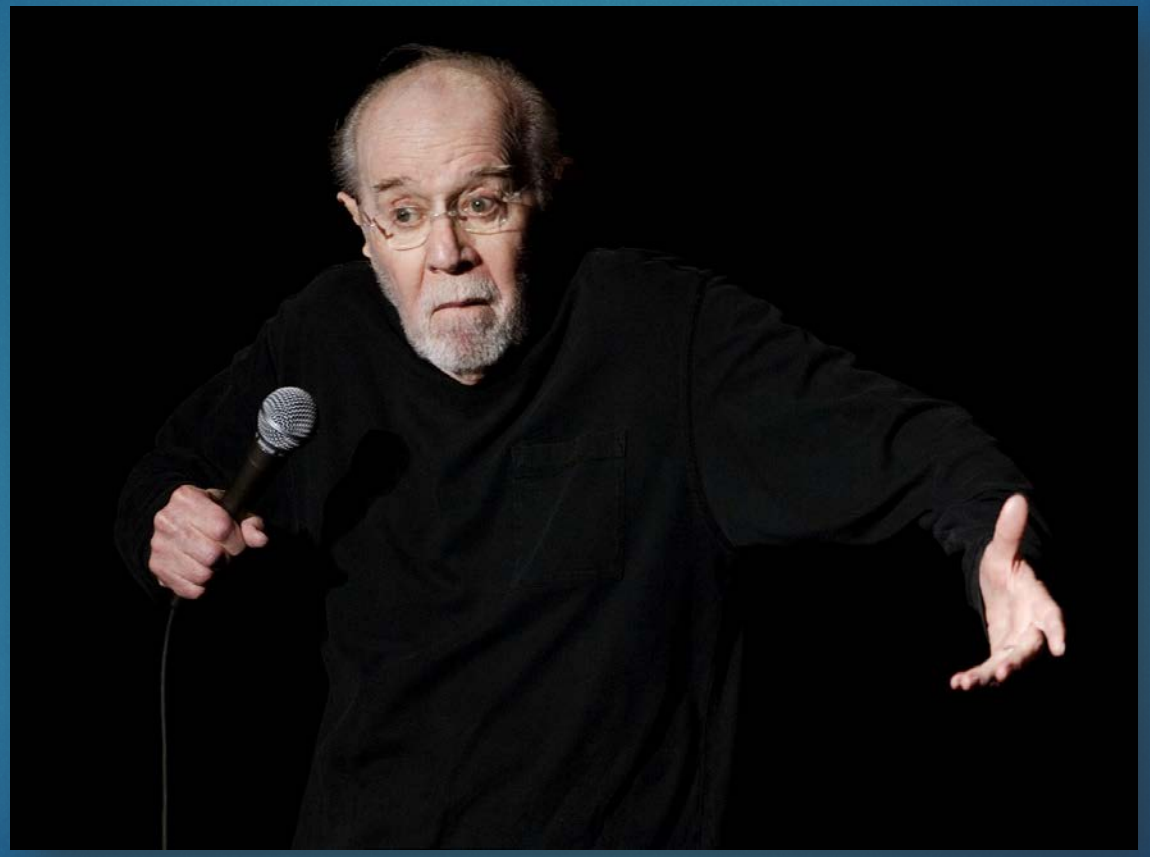
# Like a birds of a feather session


POWERPOINT

# Well, maybe a little at first

¯_(ツ)_/¯

# I’ll Set the Stage



# Then we discuss...

# …and you share your experiences and insight with the group

# But feel free to jump in…

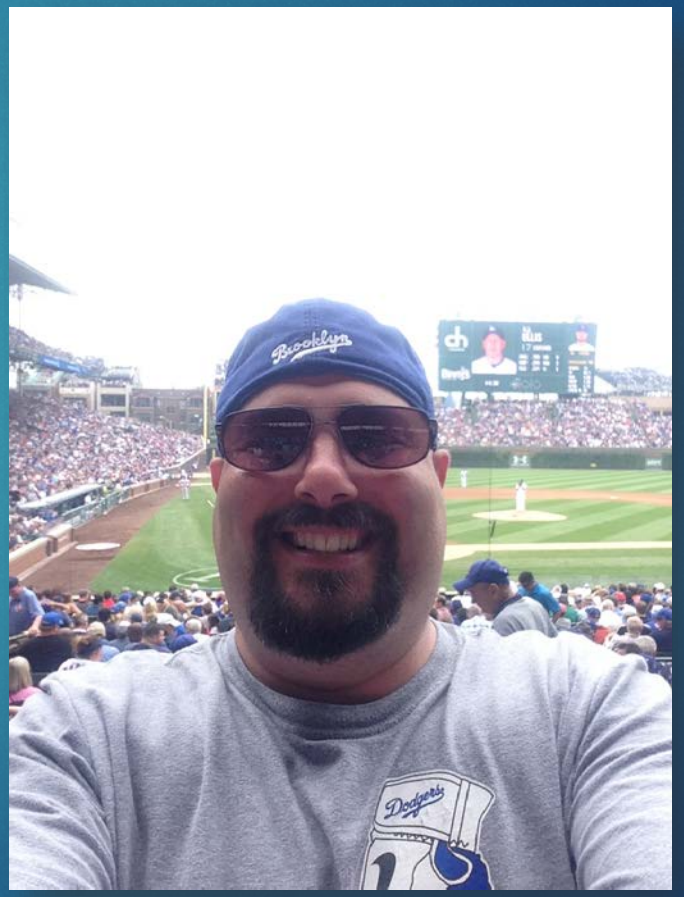
# ...if you have questions

# Disclaimer

These are my opinions and don't necessarily reflect those of my employer. Capiche?

# About me...

- Info/Cyber Security for 20 years
- Hundreds of risk assessments
- Primary developer of Calibrated Risk Index™
- Guest lecturer at VCU and UofR
- Teach CISM prep



# So I've been thinking...

# And this is probably heresy...

# A quick refresher

- Risk
  - Threat
  - Vulnerability
  - **Probability/Likelihood**
  - Impact
- Residual Risk
  - Risk factoring for mitigating controls

# Let’s do a quick thought exercise…

# Let’s attempt to figure out the probability of this risk…

- You have 10,000 active workstations on any given day
- Total number of websites in the world: 1,03B+ (as of yesterday according to internetlivestats.com)
- Your website-to-workstation ratio: 103,000:1
- Number of “bad guys” with exploit kits: ?
- Number of poisoned web sites: ?
- Number of poisoned ads: ?
- Number of users who will visit a poisoned website or get hit with drive-by ads: ?
- **Probability: ?**

# …using Single-loss expectancy (SLE)

- *SLE = Asset Value (AV) x Exposure Factor (EF)*
- *AV* = $1,000 (for the sake of argument)
- *EF* = “The subjective, potential percentage of loss to a specific asset if a specific threat is realized.” (thank you, Wikipedia)

So what’s *EF*?
How do you know?

# …using the "old" NIST way

| Likelihood Level | Likelihood Definition |
|---|---|
| High | The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. |
| Medium | The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. |
| Low | The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. |

Subjective

# …using the “new” NIST way

**LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)**

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | Adversary is **almost certain** to initiate the threat event. |
| High | 80-95 | 8 | Adversary is **highly likely** to initiate the threat event. |
| Moderate | 21-79 | 5 | Adversary is **somewhat likely** to initiate the treat event. |
| Low | 5-20 | 2 | Adversary is **unlikely** to initiate the threat event. |
| Very Low | 0-4 | 0 | Adversary is **highly unlikely** to initiate the threat event. |

**LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)**

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**. |
| High | 80-95 | 8 | Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**. |
| Moderate | 21-79 | 5 | Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**. |
| Low | 5-20 | 2 | Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**. |
| Very Low | 0-4 | 0 | Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**. |

**LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS**

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts. |
| High | 80-95 | 8 | If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts. |
| Moderate | 21-79 | 5 | If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts. |
| Low | 5-20 | 2 | If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts. |
| Very Low | 0-4 | 0 | If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts. |

**OVERALL LIKELIHOOD**

| Likelihood of Threat Event Initiation or Occurrence | Likelihood Threat Events Result in Adverse Impacts | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Low | Moderate | High | Very High | Very High |
| High | Low | Moderate | Moderate | High | Very High |
| Moderate | Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Moderate | Moderate |
| Very Low | Very Low | Very Low | Low | Low | Low |

Still subjective

# …using Monte Carlo simulation

- Uses random values to model potential results.
- Usually run thousands or tens-of thousands of times
- **Normal – Or "bell curve."** The user simply defines the mean or expected value and a standard deviation to describe the variation about the mean.
  - It is symmetric and describes many natural phenomena such as people's heights. Examples of variables described by normal distributions include inflation rates and energy prices.
- **Lognormal** – Values are positively skewed, not symmetric like a normal distribution. It is used to represent values that don't go below zero but have unlimited positive potential.
  - Examples of variables described by lognormal distributions include real estate property values, stock prices, and oil reserves.
- **Uniform** – All values have an equal chance of occurring, and the user simply defines the minimum and maximum.
  - Examples of variables that could be uniformly distributed include manufacturing costs or future sales revenues for a new product.
- **Triangular** – The user defines the minimum, most likely, and maximum values. Values around the most likely are more likely to occur.
  - Variables that could be described by a triangular distribution include past sales history per unit of time and inventory levels.
- **PERT-** The user defines the minimum, most likely, and maximum values, just like the triangular distribution. Values around the most likely are more likely to occur. However values between the most likely and extremes are more likely to occur than the triangular; that is, the extremes are not as emphasized.
  - An example of the use of a PERT distribution is to describe the duration of a task in a project management model.
- **Discrete** – The user defines specific values that may occur and the likelihood of each.
  - An example might be the results of a lawsuit: 20% chance of positive verdict, 30% change of negative verdict, 40% chance of settlement, and 10% chance of mistrial.

Source: Palisade Software & Solutions

# The Limitations of Monte Carlo

We still don't have the variables necessary to feed it

- Number of "bad guys" with exploit kits
- Number of poisoned web sites
- Number of poisoned ads
- Number of users who will accidentally surf to the wrong place

Also: "Past performance is not indicative of future results."

# What if we quit chasing our tails...


...and focus instead on threat credibility?

# Threat credibility

- If it's credible, doesn't it mean it's probable?
- Credibility factors
  - Capability/Means
  - Intent/Motivation
  - Targeting

**ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING**

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations. |
| High | 80-95 | 8 | The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions. |
| Moderate | 21-79 | 5 | The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information. |
| Low | 5-20 | 2 | The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class. |
| Very Low | 0-4 | 0 | The adversary may or may not target any specific organizations or classes of organizations. |

**ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY**

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks. |
| High | 80-95 | 8 | The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks. |
| Moderate | 21-79 | 5 | The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks. |
| Low | 5-20 | 2 | The adversary has limited resources, expertise, and opportunities to support a successful attack. |
| Very Low | 0-4 | 0 | The adversary has very limited resources, expertise, and opportunities to support a successful attack. |

**ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT**

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals. |
| High | 80-95 | 8 | The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks. |
| Moderate | 21-79 | 5 | The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends. |
| Low | 5-20 | 2 | The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft. |
| Very Low | 0-4 | 0 | The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft. |

# But I could be wrong…

# Let’s discuss