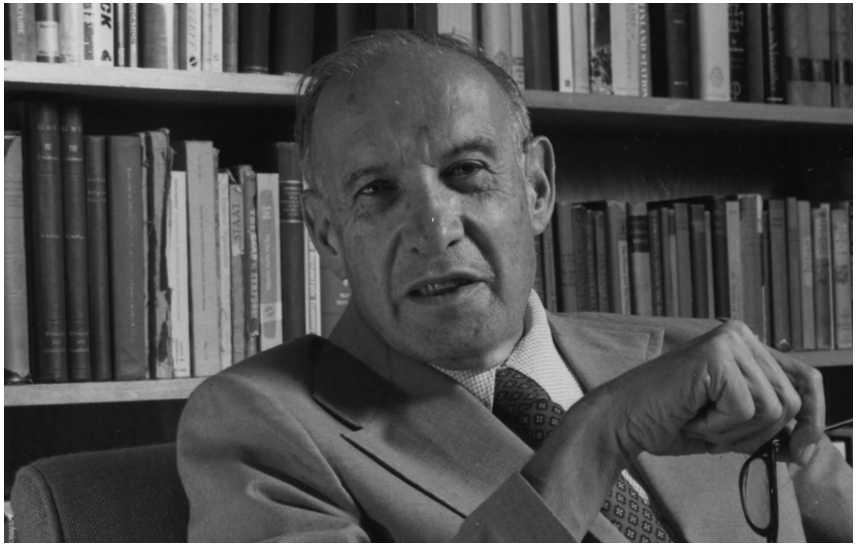
Using Metrics to Drive Improvement

Guillermo "Gil" Muñoz
Technology Services – System & Application Security
Texas A&M University

- Guillermo “Gil” Muñoz, M.A., CISSP, CEH
  Technology Services - Security Assessment
  Texas A&M – College Station

- Over 20 years in all forms of IT
  Including 13 in cybersecurity or with strong cybersecurity component
- 10 years in management, including 5 years leading software development team and 3 years in senior leadership with SIL International Papua New Guinea
- Initiated, designed and built vulnerability management processes resulting in
  - 99.7% reduction in public IP vulnerabilities
  - 91.6% reduction in vulnerabilities in internal “Key Systems”.
- Designed and built Cyber Security Integration (CSI) to integrate information from TAMU security systems (IPAM, vuln scanners, firewalls, AD, network traffic monitoring, endpoint protection, accessibility scans, etc) and to make all information available to system custodians and our security team.
- Lead for Application Security Program, carrying out mandate to implement DevSecOps/SSDLC across all software development at TAMU College Station
- Built tools for compliance scanning to ensure TAMU’s systems meet compliance and security controls.

“If you can't measure it,
you can't improve it.”

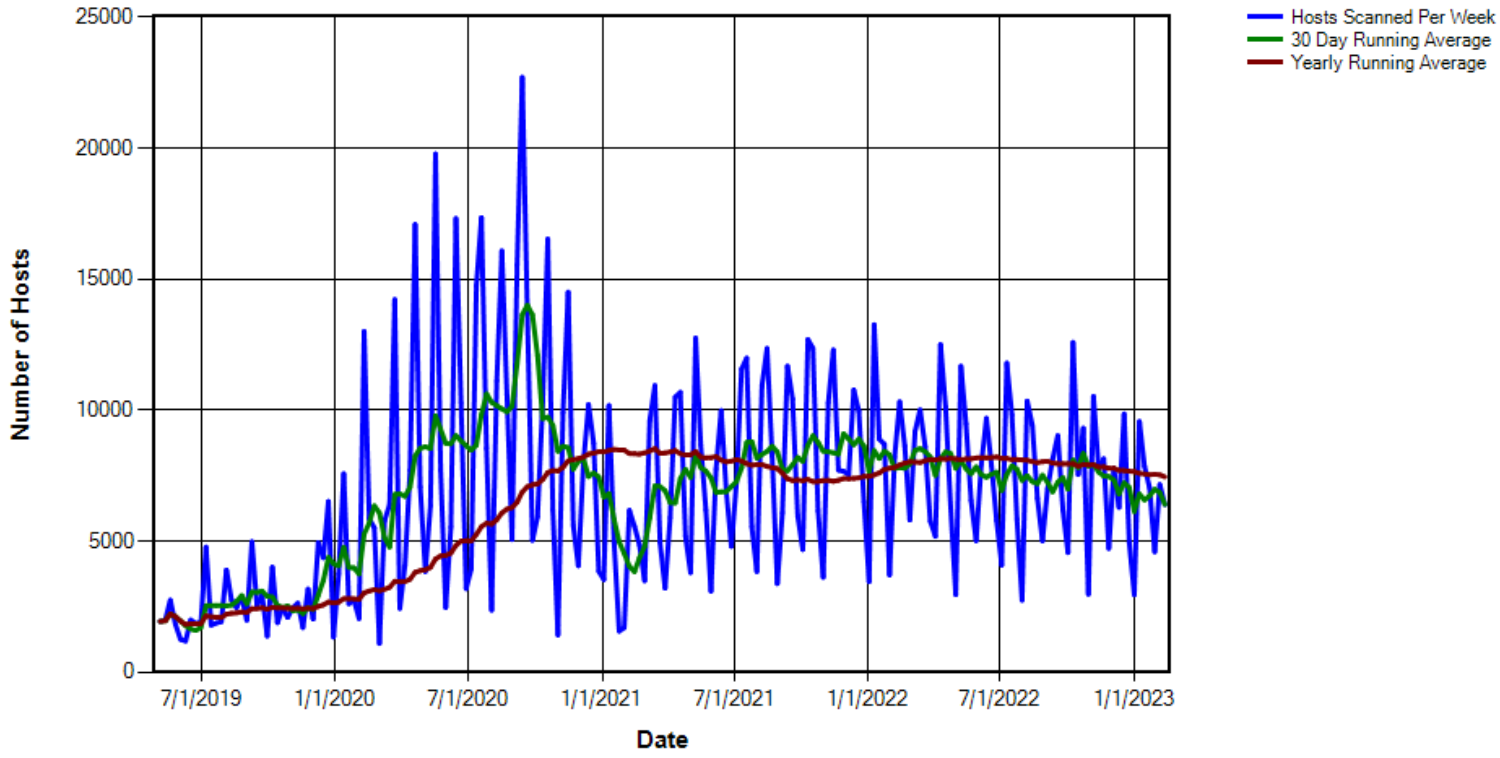


— Peter Drucker

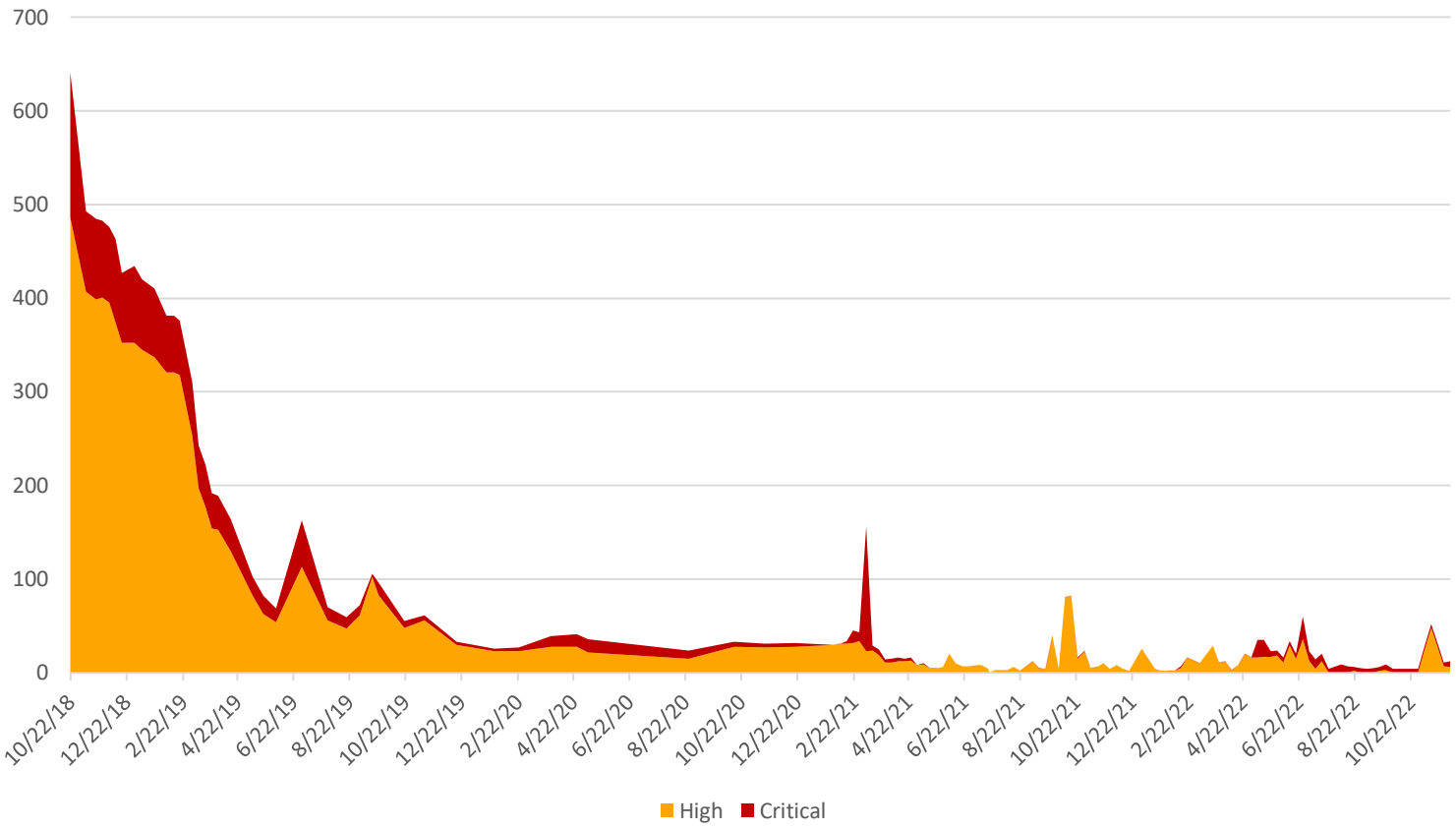
Benefits (NIST 800-55)

- Increased Accountability
- Improve Information Security Effectiveness
- Demonstrate Compliance
- Provide Quantifiable Inputs for Resource Allocation Decisions

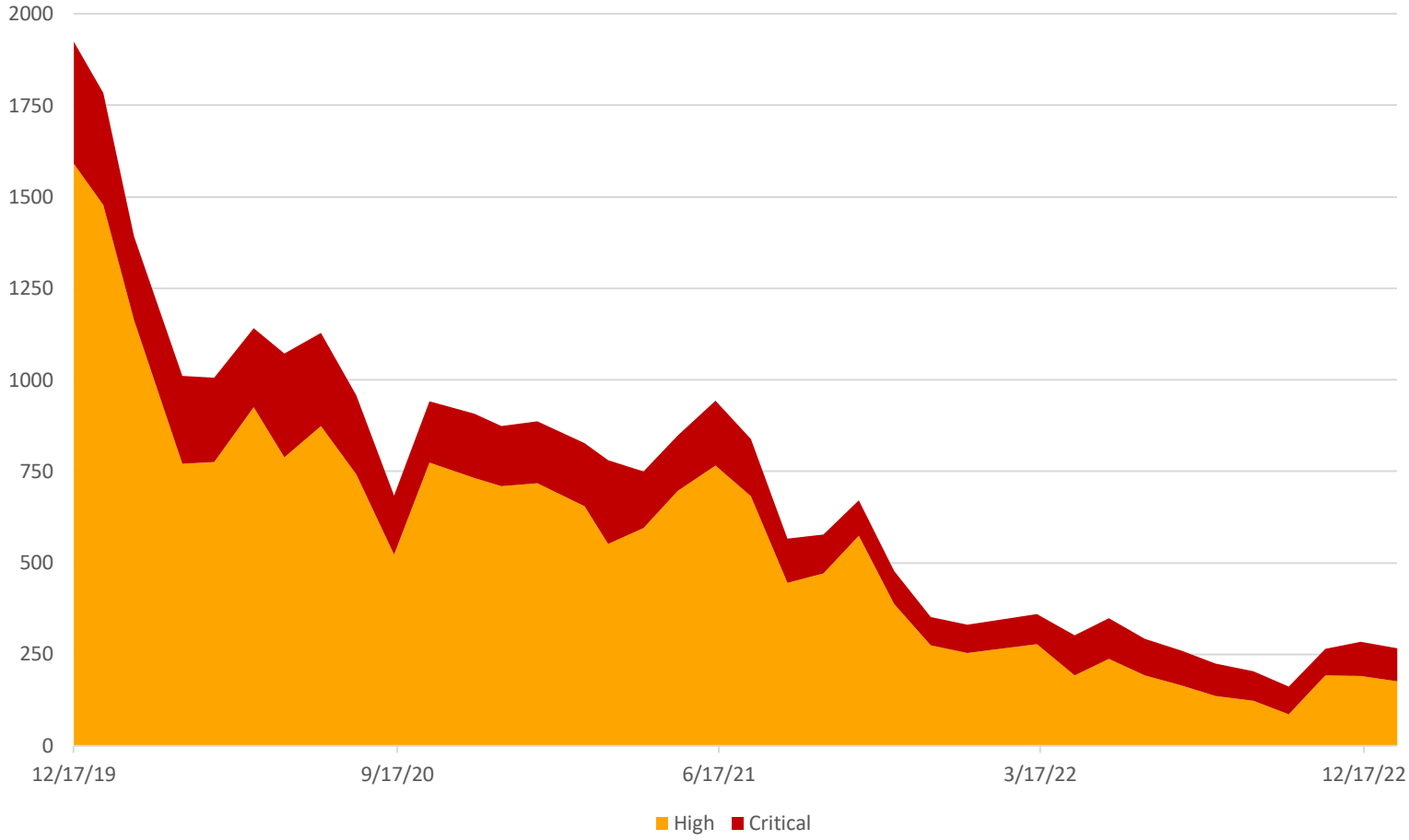
Vulnerability Scan Coverage

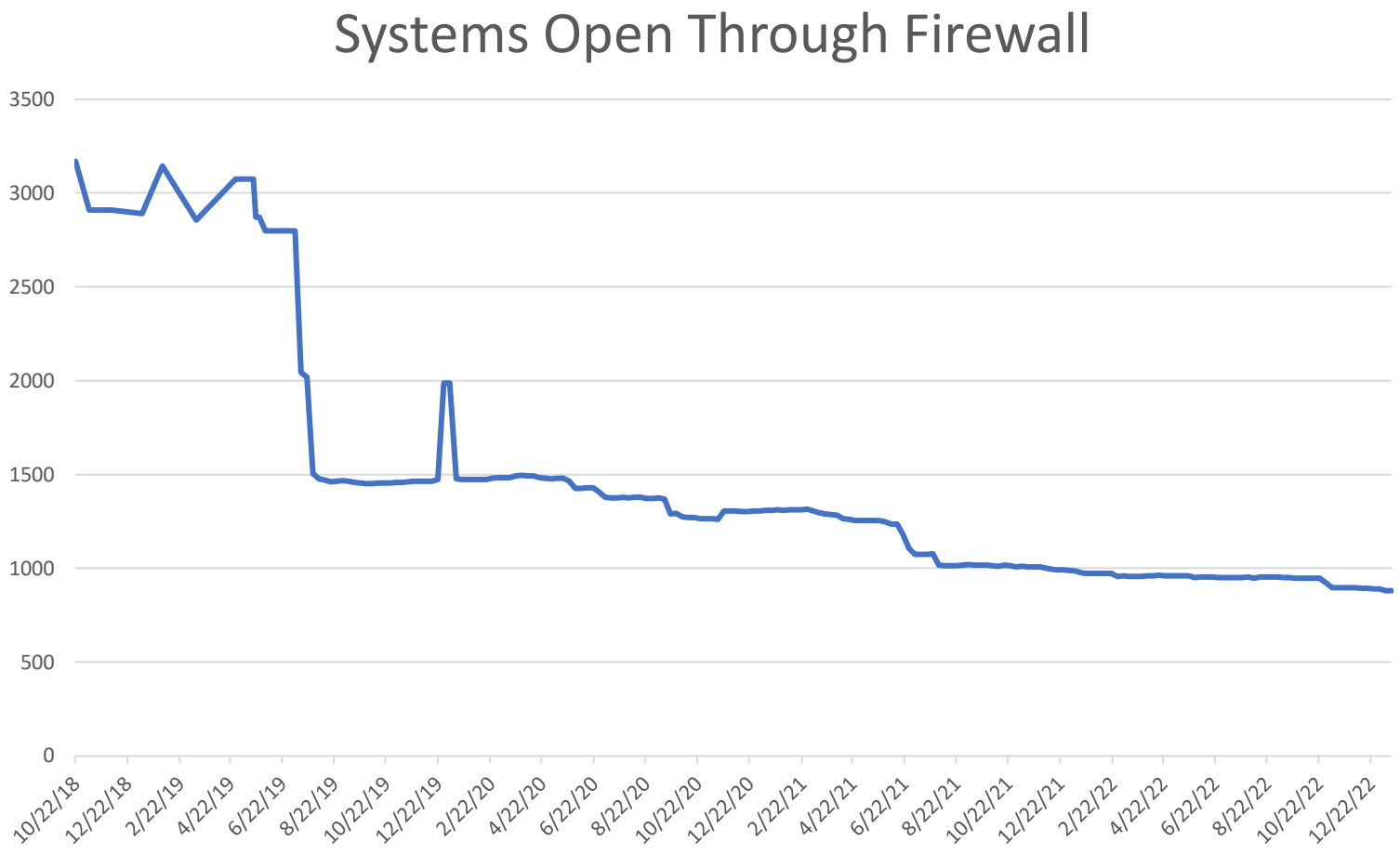


Public IPs - Exploitable Vulnerabilities

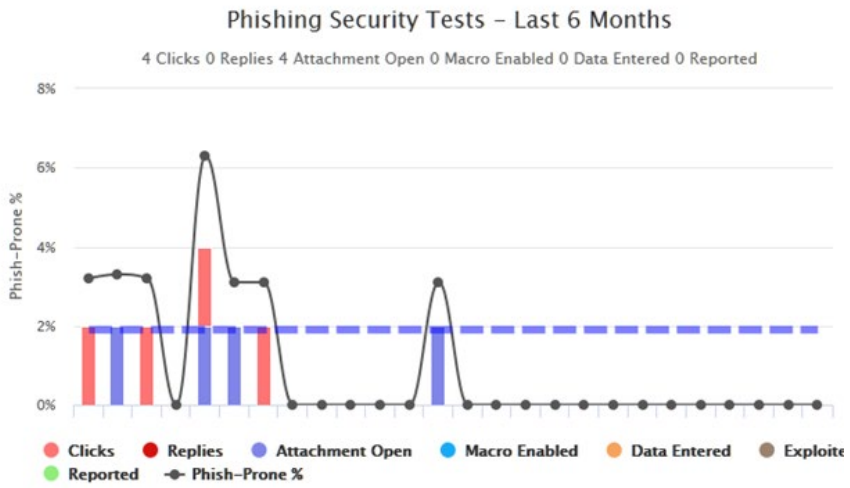


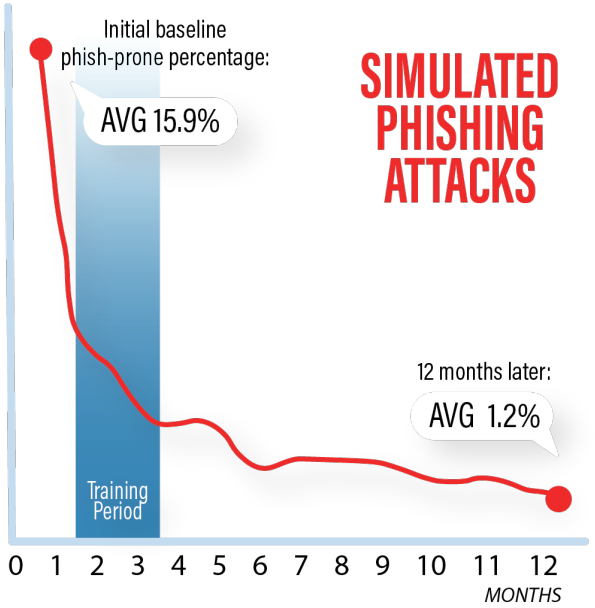
Key Systems - Exploitable Vulnerabilities




Systems Open Through Firewall
3500
3000
2500
2000
1500
1000
500
0
10/22/18
12/22/18
2/22/19
4/22/19
6/22/19
8/22/19
10/22/19
12/22/19
2/22/20
4/22/20
6/22/20
8/22/20
10/22/20
12/22/20
2/22/21
4/22/21
6/22/21
8/22/21
10/22/21
12/22/21
2/22/22
4/22/22
6/22/22
8/22/22
10/22/22
12/22/22

- Metrics vs. Measurements
  - Point in time
  - Comparison to baseline





- SMART
  - Specific – particular representation of the goal
  - Measurable – quantifiable contribution to the goal
  - Attainable – balance ambitious progress and attainability
  - Relevant – contributes to the larger mission of the organization
  - Time bound – realistic time frame

- What are good metrics
  - **Mission oriented**.
    - Don’t allow the metric to become the mission
    - Metrics should serve to advance the mission of the organization
    - Clear connection to the goals and mission of the organization
  - **Straightforward**
    - Simple and easy to understand.
    - Measurable, Objective
    - Use existing sources of information.
  - **Answer:**

    Are we more secure today than we were before?

- How to execute
  - Collect early and often
  - Be consistent
  - Stay focused – better to pick a few and really work them than a lot and not get the most out of any
  - Don’t forget metrics on team health
  - Measure responsibly
    - Bad idea to measure teams against each other
    - Use supporting metrics – gaming shows up
    - Customer focus metrics!
    - Metrics lag, use to direct future, not to punish the past
  - Communicate to right audience
  - Examine and Improve

- Categories – NIST 800-55
  - Implementation – Ex: Scanning control -> number of systems being scanned for vulnerabilities
  - Effectiveness/Efficiency – Ex: Scanning control -> number of high and critical vulnerabilities over time
  - Impact – Ex: number of breaches per year, cost per breach

- Exercise – Selecting a metric.
  - What is the mission of your organization?
  - How does your area of responsibility contribute to that mission?
  - What is the area of greatest need in your area of responsibility?
  - What are 1-3 activities that contribute the most to that area of greatest need?
  - For one of those, is there a status that can be measured, a property that reflects the status and can be quantified?

References

- Melchior, Dan. "The Fundamental Principles of Metrics | The Shared Services & Outsourcing Network." Shared Services & Outsourcing Network, 15 Sept. 2014, www.ssonetwork.com/data-management-analytics/articles/the-fundamental-principles-of-metrics.
- "5 Principles for Using Agile Team Metrics Responsibly." AgileConnection, 6 Mar. 2023, www.agileconnection.com/article/5-principles-using-agile-team-metrics-responsibly.
- "Effective Security Metrics." 6 Mar. 2023, www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/effective-security-metrics.
- Barker, Curt. *NIST Security Measurement NIST SP 800-55 Revision 1*. 2007.
- Chew, Elizabeth, et al. *Performance M NIST Special Publication 800-55 Revision 1 Measurement Guide for Information Security*. 2008.
- Hubbard, Douglas W., and Richard Seiersen. *How to Measure Anything in Cybersecurity Risk*. John Wiley and Sons, 2016.