

Security Metrics

An Overview

By Clare E. Nelson – ISSA member, Capitol of Texas, USA Chapter

This article provides an overview of security metrics as related to risk management, limited in scope to IT security.

When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science.

— William Thomson, Lord Kelvin, 1883

Information security is one of the few management disciplines that has yet to submit itself to serious analytic scrutiny.

— Andrew Jaquith, 2007

Abstract

This article provides an overview of security metrics as related to risk management, limited in scope to IT security. The selection of security metrics is critical because it costs time and money to collect and monitor the data being measured. Moreover, the choice of security metrics may lead to a false sense of security or otherwise misguide your security efforts. Hopefully this article will spur you to re-evaluate your current security metrics strategy.

At a local tavern, a CSO walks up to an actuary and epidemiologist as they discuss actuarial versus epidemiological models, plus statistical bias. The actuary and epidemiologist ask the CSO if he wants to join them. “Certainly,” he says, “I need to steal as much science as I can.”

Security metrics is a nascent discipline with more questions than answers. If someone tells you he is an expert and has all the answers about security metrics, you can bet he is wrong – unless he’s got the solid research to back it

up. Andrew Jaquith, now a senior consultant with Forrester Research, published the first definitive book – *Security Metrics: Replacing Fear, Uncertainty and Doubt* – in 2007.¹ In it he advises executives to incorporate more science into risk management by utilizing quantitative methods.

Terms

No security discussion escapes even a brief review of terms. Security is a field where confusion about even the most basic concepts thwarts our efforts. Key terms include the following usual suspects, as defined in NIST-speak per SP 800-30 on Risk Management.²

- **Security** – Information system security is a system characteristic and a set of mechanisms that span the system

¹ Andrew Jaquith, *Security Metrics: Replacing Fear, Uncertainty and Doubt*. Upper Saddle River, NJ: Pearson Education (2007).

² Stoneburner, Gary; Goguen, Alice; Feringa, Alexis (2002). *Risk Management Guide for Information Technology Systems*. NIST SP 800-30.

both logically and physically. Security goals are integrity, availability, confidentiality, accountability, and assurance.

- **Vulnerability** – A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
- **Threat** – The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
- **Threat source** – Either 1) intent and method targeted at the intentional exploitation of a vulnerability, or 2) a situation and method that may accidentally trigger a vulnerability.
- **Risk (IT-related Risk)** – Net mission impact considering 1) the probability that a particular threat-source will exercise a specific information system vulnerability, and 2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to:
 - Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
 - Unintentional errors and omissions
 - IT disruptions due to natural or man-made disasters
 - Failure to exercise due care and diligence in the implementation and operation of the IT system.
- **Risk management** – The total process of identifying, controlling, and mitigating information system risks. It includes risk assessment, cost-benefit analysis, and the selection, implementation, test, and security evaluation of safeguards.

Threats are fairly easy to understand, but risk is wide open to interpretation. The NIST definition of risk is far from simple, and evidences the dysfunction shaping the beginnings of security metrics, due in large part to different definitions of security metrics as described below. Douglas Hubbard, the author of *Why Risk Management Fails*, defines risk as “the probability and magnitude of a loss, disaster, or other undesirable event, i.e., something bad could happen.”³

Definition of security metrics

SANS, NIST, and Jaquith provide definitions of security metrics. When taken collectively, this should help you formulate the definition that suits your environment. Moreover it should give you a deeper understanding of security metrics.

To make things complicated, some authorities define security metrics as distinct and different from security measurements, while others simply refer to security measurements. NIST SP 800-55 Revision 1 standardizes on security measurements, and avoids the term *security metrics*. Note, however, that the first version of SP800-55 was titled, “Security Metrics Guide

for Information Technology Systems.” NIST defines security measurements very simply:

“Security measures facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data.”⁴

A past SANS paper⁵ quotes Jelen who defines security metrics as “derived by comparing to a predetermined baseline, two or more measurements taken over time.” Security metrics should be SMART: specific, measurable, attainable, repeatable, and time-dependent. Useful security metrics typically:

- Indicate the degree to which security goals are met
- Drive actions to improve security and comply with security policies

Examples of security metrics include the following:

- Mean-time between security incidents
- Mean-time to patch
- Risk assessment coverage
- Security testing coverage
- Mean-time to complete changes
- Percent of changes with security exceptions
- IT security spending as percent of IT budget
- IT security budget allocation

According to Jaquith, risk management is the goal, and security metrics exist to support risk management. Jaquith's definition of security metrics includes the need to classify metrics, and the acknowledgement that some security metrics are not easy to capture:

- **Security metrics** – How to quantify, classify, and measure information security operations in modern enterprise operations. Measuring security is putting numbers around activities that have traditionally been considered difficult to measure.⁶

Jaquith's security metrics guidelines are present in everything from NIST standards to academic risk management theses. He defines a good metric as:

- Consistently measured
- Cheap to gather
- Expressed as a cardinal number or percentage
- Expressed using at least one unit of measure
- Relevant to decision makers

Jaquith advocates cheap because he does not want failed ROI cases to be an impediment. He states that, in the beginning, it does not matter what you measure: just start measuring, and keep doing it. For those who are well along this path, he

³ Hubbard, Douglas W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. Hoboken: John Wiley & Sons.

⁴ Chew, Elizabeth; Swanson, Marianne; Stine, Kevin; et al (2008). *Performance Measurement Guide for Information Security*. NIST SP 800-55 Rev 1.

⁵ Payne, Shirley C. (2001). *A Guide to Security Metrics*. SANS Institute InfoSec Reading Room.

⁶ Jaquith (2007).

has tips for automating measurements and is an advocate for efficiency and disabusing bad habits. Security metrics should only be done if they support a business (risk management) decision. Avoid “happy metrics” such as “We blocked 415 threats today.”

Where is the consensus?

NIST warns against misinterpretation of security metrics:

*“An increase in the number of viruses detected by antivirus software could be a leading indicator, because the increased activity indicates an elevated threat level; but the count could also be a lagging indicator, because an efficient antivirus mechanism has been implemented. Also, decreased activity could indicate that the antivirus mechanism is losing its effectiveness, other security-enforcing mechanisms are increasingly successful, or the system is simply not being subjected to many attacks.”*⁷

Why is there a lack of consensus on security metrics? Jaquith contends it is because “the culture surrounding security is largely one of shame.”⁸ Companies that get hacked do not seek the spotlight unless forced by law. Those that have not been sabotaged keep quiet, muttering Bradford’s dictum, “There but for the grace of God, go I.”

The YouTube video, “RSA 2010: Pre-debate on Proving the Worth of Security Metrics with Real-World Data,”⁹ raises a poignant question: Are you wasting your time and money? If there is no hard data, then perhaps you are. You simply do not know, so you muddle along in sheep formation.

In his 2009 book, *Information Management Security Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*, Craig Brotby asserts, “Security metrics should tell us about the state or degree of safety relative to a reference point, and what to do to avoid danger. Contemporary metrics fail to do so. They say little about the appropriate course of action.”¹⁰ Metrics require objectives. Just because you measure, does not mean you will be secure. If you measure past behavior, how will it protect you from future mishaps?

Complexity of security metrics is increasing. We are going in the wrong direction. Brotby cites attempts by IBM and CA to integrate metrics into dashboards. He also references ClearPoint Metrics, a provider of Security Metrics as-a-Service. These may be excellent tools, but are we in danger of shaping our security metrics strategy based on the available tools, rather than science?

Although metrics and measurements are often used interchangeably, each term refers to a distinct concept. ClearPoint Metrics contends that while both measurements and

metrics are generated by direct collection of raw data from operational systems, measurements only provide magnitude. “A measurement does not provide a basis for comparison or context, and without context, you cannot make any meaningful decisions. Metrics are derived from measurements by enriching them through statistical analysis and contextual information. A metric indicates the effectiveness of your security processes, and compliance to corporate policies and legislative regulations.”¹¹

Why, Who, What, Where, When?

A discussion of the *why*, *who*, *what*, *where*, and *when* of security metrics brings clarity and further understanding because it establishes a framework for implementing a framework to implement security metrics in your organization. *How* is left as an exercise for the reader.

- **Why** – To avoid the hamster wheel of pain (Figure 1).
- **Who** – Who measures and who cares?
 - Who measures? You. Yes you, the security guy, the one who knows the difference between a honeypot and a mantrap.
 - Who cares? You, the CEO. Once your CSO reports on the state of security, you are doubly liable. Regardless of your appetite for risk, the risk management monkey rests squarely on your back.
- **What** – First, measure anything you can, later, what the models indicate.¹²
- **Where** – Depends on your risk management scope and strategy.
- **When** – Security metrics are not just for audits or certifications; integrate collection and strategy with everyday processes.

Why

Why do you need security metrics? To avoid what Jaquith calls the “hamster wheel of pain.”¹³ Figure 1 is Jaquith’s parody of the ubiquitous risk management slide. Security metrics will help you avoid the wheel by giving you a more scientific approach to making decisions and monitoring your current strategy. The goal is to be proactive instead of reactive. For example, if you fail to measure *mean-time to patch* or other patch policy compliance metrics, you may be susceptible to security incidents that could easily be avoided. If application-security-testing coverage for applications is too low, then perhaps you are more vulnerable. There are a number of security metrics that can give you an indication of your current security status and help you avoid asking, *Am I hosed?* You should know ahead of time. Of course, this is not a perfect world, and there will be occasions when you simply cannot duck to

7 Radack, Shirley (2010). DRAFT, *Security Metrics: Measurement to Support the Continued Development of Information Security Technology*. NIST.

8 Jaquith (2007).

9 David Spark here reporting for Tripwire at the 2010 RSA Conference in San Francisco – <http://www.youtube.com/watch?v=wH6zc01nv2g> (accessed 7/23/10).

10 Brotby, W. Krag CISM. (2009). *Information Management Security Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. Boca Raton: Auerbach Publication.

11 ClearPoint Metrics – <http://www.clearpointmetrics.com/Solutions/details.aspx?ParentID=15&EditID=276> (accessed on June 12, 2010).

12 Jaquith (2007).

13 Ibid.

can you confidently
answer the question,
“Who has access
to what?”

you can.

As information and data demands explode, do you have the ability to maintain control over users, their access and how they use information, while also meeting compliance requirements? Finding ways to easily and securely control your IT environments — physical, virtual and cloud — is crucial to your business success.

Consider this innovative approach — an approach we call “Content-Aware IAM”. Content-Aware Identity and Access Management (IAM) from CA Technologies gives you the control you need to confidently drive your business forward. Control identities, access and information use by going further than traditional IAM — down to the data level. You will know how data is being used and can then answer the question, “Who has access to what?”, with **confidence**.

Take control of your IT environments easily and securely. Starting here. Visit ca.com/security.

you can



avoid a bullet, but there are a number of incidents that can be avoided as a result of using security metrics instead of the “Ignorance is Bliss” approach.

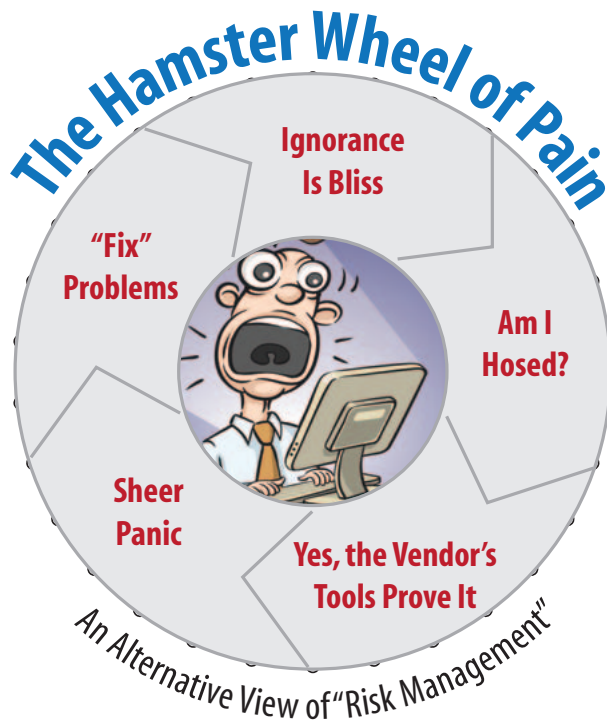


Figure 1 – The Hamster Wheel of Pain

According to Jaquith, the only reason to measure is to support risk management. “The only security metrics we are interested in are those that support decision making about risk for the purpose of risk management.”

In *The Failure of Risk Management*, Hubbard explains why many popular risk management methods are no better than astrology. His scope includes more than just security; it includes natural, geopolitical, and financial risk. Like Jaquith, he is trying to penetrate the “management market,” aiming at high-level executives as well as technologists. He believes the solution to better risk management is better quantitative analysis. Hubbard asks three questions:

- Do any of the risk management methods work?
- Would anyone in the organization even know if they did not work?
- If they did not work, what would be the consequences?

Hubbard warns against methods that don’t work. *Some of these methods become best practices and spread from one organization to the next, like a virus.* He contends that if initial risk assessment is not based on meaningful measures, the risk mitigation methods are bound to address the wrong problems. “If risk assessment is a failure, then the best case is that risk management effort is simply a waste of time and money. In the worst case, erroneous conclusions lead the organization down a more dangerous path.”¹⁴

¹⁴ Hubbard (2009).

Who

Those of you responsible for day-to-day security already know that numbers are a man’s best friends. You toil endlessly, and if everything goes right, no one notices. The bad guys have you outnumbered and outgunned; how do you maintain or grow your budget? How do you know your currently strategy is working?

Who is responsible for security metrics? The metrics may be collected by various groups, and a multitude of roles including system administrators, CISOs, CIOs, or network managers. Ultimately, one person may collect and analyze security metrics for an organization and make the data available to the groups that use the metrics as input for decision-making or course correction. For example, a CFO may be more interested in the IT security spending as a percent of IT budget. A CSO may be more interested in mean-time between security incidents. However, if one person has a unified dashboard of security metrics as depicted in Table 1, then he might have a clearer picture of an organization’s status and visibility into any areas of weakness.

What

What do you measure? If you recall Heisenberg, not from *Breaking Bad*, but from high school physics, you will easily comprehend that we can measure states or rates. Heisenberg proved you can measure the position of something, or the momentum of something. Since security metrics is such a young discipline, perhaps it is unfair to ask how the process of observing or collecting security metrics changes the observed phenomena.

What do the standards indicate? Do you care about standards? Typically, there is a subset that applies to your IT security policies. Here is a sampling of germane standards:

- NIST SP 800-39, DRAFT, *Managing Risk from Information Systems: An Organizational Perspective*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- AS/NZS ISO 31000:2009 *Risk Management – Principle and Guidelines*
- *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methods*
- *Institute for Security and Open Methodologies Risk Assessment Values (ISECOM RAV)*

The ISECOM approach advocates “no assumptions and no complex comparison, only a pure metric.” The ISECOM risk assessment values are designed to be simple, quickly calculated, accurate and realistic. “The metrics are designed to apply equally to calculating security and loss control measures for a military base, an office building, a bridge, a Mars rover, a computer network, or a single computer application.”¹⁵

¹⁵ ISECOM – <http://www.isecom.org/securitymetrics.shtml> (accessed June 13, 2010).

| CIS Security Outcome and Practice Metrics | | |
|---|--|--|
| FUNCTION | MANAGEMENT PERSPECTIVE | DEFINED METRICS |
| Incident Management | How well do we detect, accurately identify, handle, and recover from security incidents? | <ul style="list-style-type: none"> • Mean-time to incident discovery • Number of incidents • Mean-time between security incidents • Mean-time to incident recovery |
| Vulnerability Management | How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities? | <ul style="list-style-type: none"> • Vulnerability scanning coverage • Percent of systems with no known severe vulnerabilities • Mean-time to mitigate vulnerabilities • Number of known vulnerabilities |
| Patch Management | How well are we able to maintain the patch state of our systems? | <ul style="list-style-type: none"> • Patch policy compliance • Patch management coverage • Mean-time to patch |
| Application Security | Can we rely on the security model of business applications to operate as intended? | <ul style="list-style-type: none"> • Number of applications • Percent of critical applications • Risk assessment coverage • Security testing coverage |
| Configuration Management | How do changes to system configuration affect the security of the organization? | <ul style="list-style-type: none"> • Mean-time to complete changes • Percent of changes with security reviews • Percent of changes with security exceptions |
| Financial Metrics | What is the level and purpose of spending on information security? | <ul style="list-style-type: none"> • IT security spending as % of IT budget • IT security budget allocation |

Table 1 – Center for Internet Security (CIS) Security Metrics

The Center for Internet Security (CIS) gathered more than 150 government, private, and academic experts to reach consensus on an initial set of security metrics¹⁶ (Table 1).

Does hard data exist to prove which metrics reduce risk? Even if it does, how does it apply to your organization? What is the cost of adding one more metric? What is the cost of interpreting metrics? Did the CIS group of 150 consider composability? Two systems, both of which are considered to be secure, can be connected together resulting in a composite system that is not secure. Composability is a property that would lead to better security measurements; composability would allow the security measurements of small systems to contribute directly to the measurement of the larger systems of which they are a part.

Where

What is your scope? Victor-Valeriu Patriciu makes it simple to limit scope by enforcing a security metrics framework. Patriciu proposes a system for “ranking vulnerabilities in

a consistent fashion.”¹⁷ Patriciu’s framework is designed around seven base metrics that represent fundamental features of vulnerability:

- 1. Access vector** – measures whether the vulnerability is exploitable locally or remotely
- 2. Access complexity** – measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system
- 3. Authentication** – measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability
- 4. Confidentiality impact** – measures the impact on confidentiality of a successful exploit of the vulnerability on the target system
- 5. Integrity impact** – measures the impact on integrity of a successful exploit of the vulnerability on the target system
- 6. Availability impact** – measures the impact on availability of a successful exploit of the

vulnerability on the target system

- 7. Impact bias** – allows a score to convey greater weighting to one of the three impact metrics (Confidentiality, Integrity and Availability impact) over the other two.¹⁸

From these seven base metrics, Patriciu constructs a common vulnerability scoring system framework by adding temporal metrics, plus environmental metrics. In Figure 2, you can see how Patriciu maps security metrics to attacks, incidents, controls, and assets. For example, the organization’s assets, depicted in the blue box comprise of data and infrastructure. The red circle represent controls and what they do to thwart against attacks and incidents (the yellow box). For example, controls to prevent service disruption guard against denial of service attacks. The green box represents the overall security status of the organization as represented by security metrics, and poses questions:

- Is the control necessary?
- Is the control efficient?
- Are enhancements required?

17 Patriciu, Victor-Valeriu, PhD; Priescu, Justin, PhD; Nicolaescu, Sebastian, PhD Candidate; Department of Computer Engineering, Military Technical Academy, Bucharest, Romania. “Security Metrics for Enterprise Information Systems.” *Journal of Applied Quantitative Methods* 1(2):151-159.

18 Ibid.

16 Center for Internet Security – <http://cisecurity.org/en-us/?route=downloads.metrics#progress> (accessed on June 11, 2007).

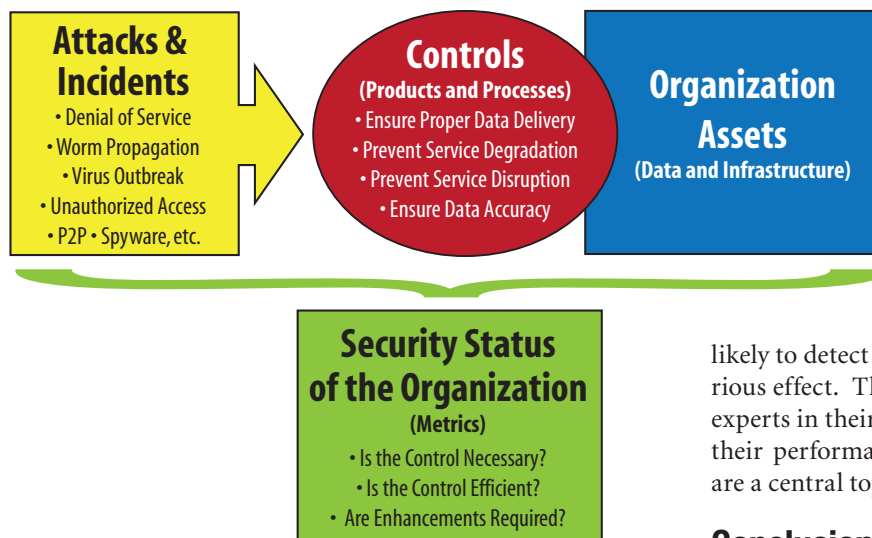


Figure 2 – Patriciu's Network and System Security Based on Metrics

These questions imply a continuous refinement process. Note that the first question is whether or not a control is necessary. However, a control that is necessary today may not be necessary, or sufficient, tomorrow.

Patriciu echoes common sources for error: unclear definitions, flawed models, people (who are innately biased), institutional isolation, and inertia to change.

When

When do you collect security metrics? How often do you assess them? The answers to these questions are based on the risk management and security policies. Once you get a system in place and collect security metrics on a regular basis, some metrics may need to be measured more often, especially those related to incident management. Metrics related to finance and budget allocations may align with your unique budget cycles. Jaquith urges people to adopt security metrics practices with consistency and discipline. According to SANS there are three critical queries, and the periodicity for collecting security metrics may be gauged in part, by how well these queries are addressed:

- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secure enough?¹⁹

Experts or metrics?

Who is best qualified to answer the SANS critical queries above? Are *expert* opinions the best? According to Hubbard, they are dangerous at any speed. He refers to research to back up his statements. Hubbard contends that expert training increases confidence while making judgments worse. For example, security experts have a high degree of confidence, even when their judgments are wrong. Hubbard explains that

the people-factor in risk management needs to be calibrated and people need to be re-trained to account for their bias. He calls for a 180-degree U-turn to set things right.

A recent Hubbard blog guest post comments on the “placebo effect” in decision making. “According to studies, receiving formal training in lie detection (e.g., so that law enforcement officers are more

likely to detect a untruthful statement by a suspect) has a curious effect. The training greatly increases confidence of the experts in their own judgments, even though it may decrease their performance at detecting lies.”²⁰ Such placebo effects are a central topic of *The Failure of Risk Management*.

Conclusion

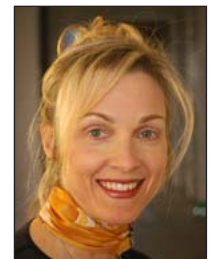
To reiterate Jaquith's assertion, security metrics exist to support risk management. Ideally, your security metrics guidelines will define the *who, what, where, why, and when* of security metrics. From a management perspective, security metrics can help determine the level and purpose of spending on information security, as well as track and understand the technical aspects of security as it relates to risk management. The field of security metrics, while young, is evolving. As CSOs adopt a more documentable and scientific approach, look for security metrics to take more of the spotlight. Hopefully this paper gives you a basic understanding of why terms such as security measurements or security metrics are used by different standards organizations. The initial set of security metrics gathered by CIS, in Table 1 is an excellent start if you are establishing a security metrics strategy for your organization.

References

- Bushmiller, Dean (2010). *Security Metrics*. UT Austin, Expanding Security, Inc., Security Summit.
- Cox, Mark. YouTube, “Mark Cox, episode 4. Security issues and metrics.” <http://www.youtube.com/watch?v=rbpaqUuS844> (accessed June 13, 2010).
- Geer, Daniel (2006). PowerPoint: Measuring Security. Geer Risk Services, Cambridge.

About the Author

Clare E. Nelson, CISSP, is founder and CEO of ClearMark Consulting, LLC. She has been in high tech for over thirty years, spanning software engineering (encrypted TCP/IP variants), product management (storage, system management), and business strategy. Clare holds a BS in Mathematics from Tufts University. She may be reached at nclare@austin.rr.com or [Safe_SaaS](#) on twitter.



19 Payne, Shirley C. (2001). *A Guide to Security Metrics*. SANS Institute InfoSec Reading Room.

20 Hubbard, Douglas – <http://blog.hubbardresearch.com> (accessed June 12, 2010).