ALICE AND THE PATENT BEAST

INTELLECTUAL PROPERTY AND ECONOMIC PROSPERITY: FRIENDS OR FOES?

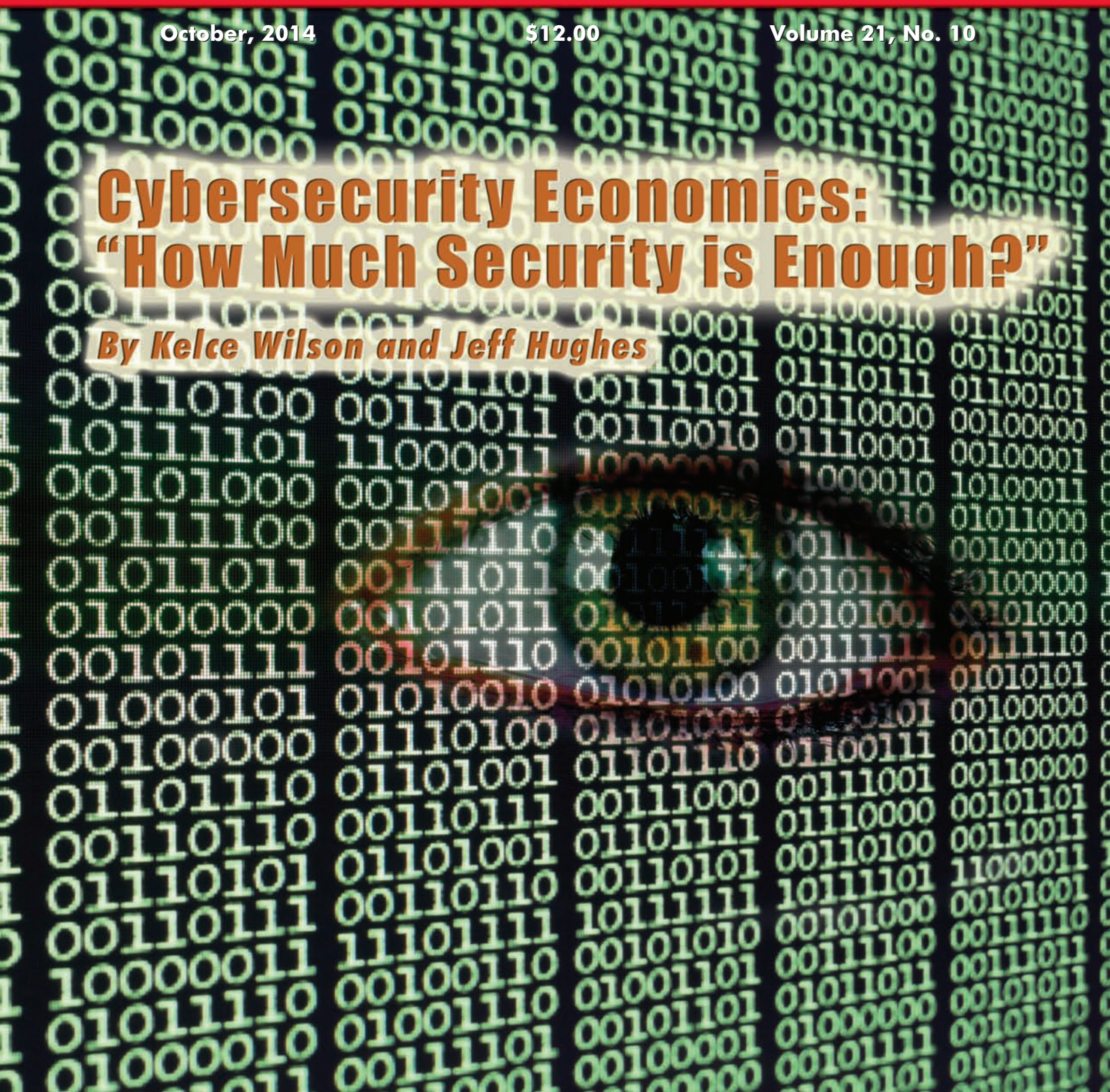
NEW I.P. LAWSUITS – RFCEXPRESS.COM

Intellectual Property Today™

www.iptoday.com

A Publication of Omega Communications

October, 2014 $12.00 Volume 21, No. 10



Cybersecurity Economics: "How Much Security is Enough?"

By Kelce Wilson and Jeff Hughes

Cybersecurity Economics: "How Much Security is Enough?"

BY KELCE WILSON AND JEFF HUGHES

Mr. Hughes may be contacted at: jeff.hughes@tenet3.com

It may be inevitable that your firm or one of your clients suffers a serious data breach — despite efforts to remain current with the latest protection systems. When that happens, will you have a convincing argument, based on objective and technically sound criteria, that you or your client had expended reasonable efforts to maintain data security? Or, will accusations of negligence be more convincing and set the tone for post-incident sanctions and penalties?

You can't provide a convincing defense if you had no basis for defining what a reasonable level of effort should have been prior to the incident. So ask your clients and inquire around your firm, have your panic attack when you find a dearth of objective criteria, and then read on to find a solution.

Law firms, just as public and other private sector organizations, struggle to determine what cyber security investments are appropriate and beneficial in protecting the critical parts of their business operations. Managers of large information technology (IT) systems make policy and technology choices on a regular basis that impact both their users' experience and their system's confidentiality, integrity, and availability. Lacking empirical data, these choices are often made using mere (allegedly) expert opinion. Dependencies and competing interests from processes (policy manifestations) and mechanisms (technology manifestations) complicate the choices. Security at the strategic enterprise level and at the tactical component level has typically been implemented without guidance from a rigorous, quantitative risk assessment and mitigation methodology.

Straightforward questions such as "How much security is enough for the threat we face?", "What are our residual risks?", and "Does this security investment provide benefits worth the costs imposed?" need straightforward answers. Our approach to providing those answers and performing necessary due diligence is outlined herein.

CYBERSECURITY MARKET FUNDAMENTALS

Law firms are increasingly being advised of the need for a comprehensive cybersecurity and threat mitigation plan as part of their overall risk management approach. The costs of not performing cybersecurity due diligence are high with penalties looming based on statutes and ethical liabilities. Yet, designing, deploying, monitoring, and maintaining a solid cybersecurity solution has been challenging to date due to three market fundamentals.

First, cybersecurity is more than a function of the types of information technology (IT) employed by your firm. It is also a function of business processes (both required and latent) and personnel cyber-related work habits (both good and bad). Security "best practices" can often be at odds with efficient firm operations. This complex and competing mix of technology, processes, and personnel is a principal reason why achieving a reasonable cyber risk profile can be challenging.

Second, new IT technologies introduce new vulnerabilities. Did you ever ask yourself: "Why can't they just fix security once and for all?" New software and hardware inevitably have new bugs. Current information systems strive for high levels of information availability, so you can access information wherever you are, any time you need it. Unfortunately, the availability of our always on and always connected work environment often trumps important confidentiality and data integrity concerns. There are best practices for writing secure code and fabricating trustworthy hardware, but "time to market" and global economies of scale make these security practices a languishing desire, especially when the economic trade space of residual risk versus security implementation costs is unclear.

Third, you can't fix what you can't measure. Historically, there has been a lack of fundamental metrics to guide our way in understanding the cybersecurity cost/benefit trade space. The authors and their colleagues have made fundamental advances in cybersecurity metrics[1,2,3,4] over the past few years. Yet there is still an extensive reliance on point solutions and static compliance checklists, instead of preferable dynamic threat mitigation strategies that are evaluated on an ongoing basis using quantitative metrics.

CURRENT STATE-OF-THE-ART GUIDANCE IN CYBER RISK MANAGEMENT

The National Institute of Standards and Technology (NIST) recently published details of a Cybersecurity Framework Core in response to directives in the February 2013 Executive Order 13636: Improving Critical Infrastructure Cybersecurity. In this NIST security document here are 5 principal functions necessary to implement a strong security methodology: identify, protect, detect, respond, recover. Associated with these 5 functions are 22 activity categories; 98 subcategories; and 224 possible security controls to apply. Controls are prioritized as P1, P2, P3, and P0 (P1 meaning "priority one" and P0 meaning no priority specified). Out of the 224 itemized security controls, 121 controls are labeled as P1.

The NIST Framework is solid guidance and thoughtfully prepared by some of the nation's most savvy cybersecurity experts. IF properly and extensively applied (that is a big "IF"), it can help with designing a very secure IT system. However, it still boils down to your organization's risk mitigation strategy, for which you must decide how many and which of the security controls should be implemented.

Despite the availability of the NIST guidance, you are still left with answering the burning question: "How much security is enough?"

The National Security Agency (NSA) also provides some guidance on cybersecurity matters through efforts relating to information assurance (IA). The NSA had endorsed the concept of five pillars of IA. These are availability, integrity, authentication, confidentiality, and non-repudiation. We have found that they are not independent; availability can introduce conflicts with confidentiality and integrity.

The goal of availability is to ensure or preserve access, whereas the goal of confidentiality is to prevent discovery by users who lack proper authorization and the goal of integrity is to prevent modification without proper authorization. When an authorization attempt experiences a false alarm

and improperly shuts off access, confidentiality frustrates availability. Conversely, attempts to maximize availability (perhaps by making too many back-up copies or loosening access requirements) may result in failures of confidentiality or integrity measures.

CYBERSECURITY ECONOMICS

The defender of a computing resource, typically the owner, has multiple competing requirements to satisfy. First, the system cannot be hamstrung by security. The system must support business needs by providing a useful capability (where usefulness is often characterized by availability, adaptability, and extensibility). Second, the defender must protect the system (and hence the business) against multiple adversaries. The defender's resources are spread amongst these competing objectives with the hope that defenses have been optimally applied to secure the system..

In contrast the system's *insecurity* is expressible as information arbitrage practiced by the attacker (i.e. the attacker knows something the defender doesn't and profits by it). This delta knowledge is achieved in a variety of ways, but fundamentally it boils down to time spent by the attacker to learn the weaknesses of the target system and develop an exploit.

The adversary gains this knowledge by both observing the defender's system over time and practicing their attacks on similar systems or components that are often commercially available. The attacker typically has a limited set of objectives which aids in focused application of his resources.

The defender only becomes aware that an attacker/defender information differential existed when a system vulnerability is internally discovered, published by others, or worse yet, demonstrated by the adversary. Hope is not a defensive strategy — identifying, tracking, and mitigating opportunities for information arbitrage is.

The economic equation surrounding this information arbitrage can be simply stated, as "time is money". To gain knowledge, the attacker must expend resources just as the defender does. Cybersecurity economics largely depends upon:

- Time spent by the attacker to identify, analyze, and ultimately crack the target system
- Time spend by the defender to deploy the system, maintain it, and recover from an attack

By analogy, the concept of "time-to-compromise" a physical security system is an accepted and measurable performance metric (for example, the length of time it takes to break through a vault door). The amount of physical security you employ is based on your estimate of the persistence of likely attackers. Similarly, using our framework below, we can estimate resources expended by both attacker and defender. We use quantitative cybersecurity metrics grounded in *time* because they are essential to developing rational security cost/benefit trades and clarifying your firm's level of reasonable cybersecurity investment.

A QUANTITATIVE FRAMEWORK TO CAPTURE THE "TIME IS MONEY" TRADE SPACE

Our framework is based around a classical threat characterization and decomposition model, an instructive threat mitigation methodology grounded in military strategy, and quantitative *time* based performance metrics. The framework highlights appropriate system measurements to generate the quantitative data to feed metrics and inform strategies. These metrics may be either absolute or relative, but in both cases they are quantitative "assessments of goodness" or "figures of merit". The metrics enable security trend analyses for your organization's architecture.

Furthermore, the metrics inform cost/benefit trade space analyses applicable to risk mitigation plans or continuity of operations plans. The metrics support analyzing "as designed" versus "as operating" instances of an IT system. The framework enables computing the performance and knowledge delta between cyber technology mechanisms and human processes. Finally, the framework supports quantifying adversary work factor, especially in the context of so-called "Moving Target Defenses" to increase work factors and better defend systems.

Characterizing the Threat

The first step to understanding your system is to do what nation state class threats do: Perform an "all source intelligence" action. Gather as much associated documentation as possible to determine potential susceptibilities. Typical enterprise IT systems are built from widely available components, so developing insights into system operations is greatly facilitated. All systems will have design trade-offs that result in inherent weaknesses. No real-world system can exist that provides complete availability, integrity, and confidentiality. These core information assurance goals are in fact antithetical, so that trade-offs between them are necessary to arrive at a workable system. Moreover, systems contain unintentional design or implementation flaws. The threat's goal is to discover and exploit these susceptibilities.

The second step is to identify access points into your system. A threat will probe and analyze a system in order to discover which susceptibilities are accessible and could therefore be exploitable. Generally, the threat will use access points or services that are offered to legitimate users as the initial point of entry into your system.

Finally, after a thorough surveillance, an attacker will typically employ a methodical exploitation approach, during which they expect to observe certain system responses. These system responses serve as exploitation guideposts and significantly aid the attacker. The degree to which the attacker is successful will depend on their level of system knowledge (information arbitrage), their ability to access the system, and their overall capabilities to observe and exploit vulnerabilities.

Hence, our working threat model is built from these three actions: 1) identify likely system weaknesses; 2) enumerate all user access points; and 3) list the minimal threat capability needed to exploit weakness, given the access point. A total resulting system vulnerability is then determined, based on the intersection of susceptibility, threat access, and threat capabilities.

Our threat model supports reasoning about whether an inherent system weakness rises to the level of a de facto vulnerability that must be addressed. This is in stark contrast with those who try to deal with all weaknesses as de jure vulnerabilities. This distinction is essential for cost effective risk mitigation and sensible prioritization of resources.

Additionally, our threat model enables an explicit work factor analysis and is an essential starting point in assessing a firm's risk profile. Breaking the threat into these addressable components offers choices to IT system security designers and enables cost effective trades between different threat mitigation strategies.

The Three Tenets: Addressing a Threat's Time-to-Compromise

Our security engineering methodology is called the Three Tenets; the US Department of Defense (DoD) has documented the Three Tenets as an emerging

cyber security metric. When applied, they directly impact the threat by minimizing each element of the threat model (minimize susceptibility, access, and threat capability). They are consistent with NIST guidance and the NIST cybersecurity framework. The Three Tenets methodology offers an innovative testable path forward to threat-driven and quantitative cyber metrics, since they directly modulate the adversary work factor.

The Three Tenets are:

1) Focus on what is critical

a. Focus your defensive resources.
b. Remove system components not necessary for the mission at hand (potential susceptibilities).
c. Minimize access points, thereby limiting what you have to watch.

2) Move "Out of Band"

a. Differentiate between threat access and user access.
b. "Stand" beyond the reach of the threat to watch your system.

3) Detect, React, Adapt

a. Implement sensors to automate the acts of watching and responding.
b. Have a plan of action when alarms sound (including false alarms).
c. Re-assess your security concept of operations (CONOPS) frequently; update them based on the threat; make yourself a moving target.

The Three Tenets comprise a classic military stratagem; all three are important. Tenet 1 activities limit system susceptibilities through system design choices, construction, and maintenance. Tenet 2 encourages modifying the utility of a system access point in favor of the authorized user and in disfavor of the threat. Cryptography is the best example of this, however, other access modifications can be implemented which provide strong differentiation between the user and the threat. Tenet 3 should typically be thought of as an active countermeasure, a sensor with a programmed reaction, a mechanism that does not require a human in the loop. When properly implemented, the Three Tenets produce a significant increase in adversary work factor.

Threat Driven Metrics: Compute Defender versus Adversary Work Factor

We are all familiar with quoting a job based on the number of person hours necessary to complete it. By analogy, this concept we call "work factor" can be either absolutely or relatively related to the time spent to defend or attack a system.

Consider, for example, the case of US government General Services Administration approved Class 5 security vault doors that are suitable for storing national security information. These doors must provide protection against unauthorized entry for the following periods of time:

- 20 man-hours surreptitious entry
- 20 man-hours against manipulation of the lock
- 20 man-hours against radiological attack
- 30 man-minutes covert entry
- 10 man-minutes forced entry

The point of this example is to illustrate why our threat model (susceptibility, accessibility, capability) is an informative way to decompose security. The system weakness (susceptibility) is the door construction. The access point is understood to be physical access to the door. This access has been modified and is temporarily "out-of-band" to the attacker due to their lacking the lock combination. Hence the attacker has to focus on the listed types of attacks to circumvent this knowledge gap. The difference in the attacker's capability directly relates to how quickly they can break in. Application of the Three Tenets modulates the attacker's ability to identify weaknesses, locate access points, and perform exploitations.

Our methodology allows us to estimate relative time-to-compromise for cyber systems and compute metrics related to work factor. We can also compare adversary work factor to defender work factor. Defender work factor can be estimated by examining "time to protect" and "time to maintain once protected". Adversary work factor can be estimated by analyzing "first time to break" versus "n^{th} time to break" for multiple system instantiations. (Note that threats learn and improve skills over time, so a subsequent break may be quicker.) These and other work factor estimates can be evaluated on an ongoing basis to support continuous monitoring of your defensive measures.

ESTABLISH YOUR FIRM'S CYBERSECURITY INVESTMENT PLAN

Developing cogent models describing the interplay between system operation and maintenance, security, and human user incentives is critical to informed risk mitigation and cost/benefit analyses. Economic models of security should provide a trade space where one can evaluate system use incentives and security strategies that align business benefits with the public good. A cyber attack continuity of operations plan is essential for any business and should answer these questions:

- What is absolutely critical to your firm's operations?
- Do you monitor your system's "as planned" versus "as operating" critical functions?
- Do you have a continuity of operations plan that continually adapts for changing threats?
- What is the minimum acceptable estimated time to break, based on the value of data we hold?
- What is the minimum acceptable attacker skill level, based on the value of data we hold?

The framework outlined above can support you in answering these questions. And in the process, you'll be able to model the mix between your firm's technology and human based processes. Monitor both personnel habits and institutional habits. Identify and analyze your availability versus integrity versus confidentiality tradeoffs and understand the seams in your security posture. You'll be able to track your firm's cybersecurity investments and, with documented due diligence, to answer the critical questions: "How much security is enough?" and "Can we convincingly say that we have implemented a reasonable level of security?" IPT

ENDNOTES

1. J. Hughes and G. Cybenko. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*. August 2013: 15-24.
2. J. Hughes and G. Cybenko. Three Tenets for Secure Cyber-Physical System Design and Assessment, SPIE DSS, 2014, Baltimore, Maryland.
3. Lawrence Carin, George Cybenko, Jeff Hughes. Cybersecurity Strategies: The QuERIES Methodology, IEEE Computer Magazine, Vol. 41, 2008.
4. Kelce Wilson. An Introduction to Software Protection Concepts, Intellectual Property Today, August 2007.