

**Toward Evidence-Based Information Security Practice:  
The DOE Science Community's Opportunity  
for Real World Information Security Operations Research**

Responsive to Focus Area 3: Trust within Open, High-End Networking and Data Centers

Craig Jackson

[scjackso@indiana.edu](mailto:scjackso@indiana.edu)

Center for Applied Cybersecurity Research - Indiana University

---

With so many organizations struggling to identify, much less meet, baseline levels of information security, the DOE science community has an opportunity to support and contribute impactful, real world research to understand and improve operational security. Existing social science research methods, when expertly utilized, hold tremendous promise in helping us understand information security practice *in situ*.

**1. We are struggling to find explanations and solutions for even the most mundane attacks and obvious defensive shortcomings.**

Many of the most frequently successful and negatively impactful information security attacks hinge on attacker methods that are frustratingly simple and even more frustratingly persistent. For example, a 2012 report claimed that 91% of targeted attacks utilize spear-phishing to gain access to user credentials and/or gain a foothold in victim networks.<sup>1</sup> The DOE science community, like the rest of our society, has a well-documented history of struggle with attacks like these.<sup>2</sup> At the same time, many of the most high profile (and potentially high impact) attacks leverage obvious shortcomings in defenders' information security programs (*e.g.*, unsegregated networks, untrained personnel, unpatched software). At first glance, a reasonable observer would expect there to be simple solutions to what appear to be simple problems. Why can't we systematically beat spear-phishing with technical safeguards and user training? Why aren't organizations successful in training their personnel on security policies and good practices? Security practitioners can guess at answers, and try out different solutions. When trial-and-error fails, it only makes sense to take a more systematic look at the phenomena in question.

**2. The DOE research community and society in general will benefit from systematic research into information security practice *in situ*.**

Much of the challenge to finding real world information security solutions lies in the fact that the security community lacks anything like an evidence-based, systematic understanding of security practices *in situ*. When the proverbial *rubber* of security standards and "best practices" meets the *road* of actual security practice and human behavior, security controls come into contact not only with the adversary, but also with each other, organizational governance, interpersonal relationships, yearly budgets, and the fact that most of our individual and group missions involve something more productive than security.

---

<sup>1</sup> Trend Micro Incorporated, Spear Phishing Email: Most Favored APT Attack Bait, 2012. Available: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf>

<sup>2</sup> Top Federal Lab Hacked in Spear-Phishing Attack, Kim Zetter, WIRED, 2011. Available: <http://www.wired.com/2011/04/oak-ridge-lab-hack/>

Doctors rely on medical research to inform their practice, just as medical research relies on doctors and hospitals to study what happens to real patients facing health challenges. Contemporary security professionals are like pre-Enlightenment doctors, learning their craft from peers and mentors, without the benefit of science and organized approaches to accrete, test, and disseminate knowledge. Much of the security knowledge in the wild is neither based in recognized research methodologies nor sufficiently documented to make successful security programs reproducible.

We need systematic research into real world security practice, to derive reliable descriptions of how attacks and controls play out in real world situations, as well as generalizable knowledge regarding the methods that lead to successful defense and the factors that decrease and increase the likelihood and impact of incidents. Too often, we don't know enough about an activity in the actual environment in order to know where and how to innovate. Good descriptive research is the foundation for evidence-based standards and practices, as well as R&D. Focus Area 3 calls for "performing research to ... understand the resilience of DOE scientific computing to integrity failures ... [and] create the means for developing coherent authorization and access controls particular to the open science mission." This statement rightly points out that we may not be ready to develop coherent authorization and access controls, and that we do not understand the nature of resilience in our operational environments. Others have made strong cases for the need for a *science of cybersecurity*<sup>3</sup>, but too narrow a methodological focus (e.g., on computer science methods) will hinder the speed and scope of progress. A prerequisite to confident solutions is an accurate descriptive understanding of how and whether existing and past approaches work in the real world.

### **3. We have to look outside the security community for methodological expertise in research methods.**

There are many ways to systematically study security phenomena *in situ*, but the security community must elicit help. We too frequently see information security as a technological challenge, and too often believe that reasoning, experience, and ingenuity can produce reliable solutions to our security problems. The social sciences and other fields with well-established research-to-practice traditions (e.g., education and medicine) hold more than the promise of clever analogies: They offer serious research methods, refined over decades, designed to develop and test knowledge of real-world phenomena.<sup>4</sup> Anthropology, psychology, education, and sociology (to name a few domains) have considerable expertise in the use of surveys, interviews, questionnaires, tests, scales, and observational methods, as well as ways to reliably analyze both quantitative and qualitative data. In many cases, where these methodologies are being used to produce publicly available information security research, it is in the context of events that happen outside or across our organizations' gates (e.g., cybercrime) or with research samples of 'average users' or 'consumers.' However, these powerful methods can and should be leveraged to understand organizational, operational security, and to build knowledge in the public domain. We should not only be securing funding streams for social, behavioral, and economic research into information security<sup>5</sup>, but actively recruiting top social scientists to assist security researchers and organizations in answering our security questions regardless of funding source.

---

<sup>3</sup> Fred B. Schneider, *Blueprint for a science of cybersecurity*, The Next Wave, Vol. 19 No. 2, 2012. Available: <https://www.cs.cornell.edu/fbs/publications/SoS.blueprint.pdf>

<sup>4</sup> For a primer, see, e.g., Colin Robson, *Real World Research*, 3rd Edition, 2011.

<sup>5</sup> A task seemingly increasingly difficult to achieve. See, e.g., House bill slashes research critical to cybersecurity, *Computer World*, April 22, 2015. Available: <http://www.computerworld.com/article/2913657/cybercrime-hacking/house-bill-slashes-research-critical-to-cybersecurity.html>

#### **4. The DOE science community has an opportunity to support high-impact research into real world, generalizable security practice.**

DOE ASCR may have a special opportunity both to contribute to the security of DOE facilities and DOE-funded missions, and make more generalizable contributions to our society's understanding of information security practice. Private sector organizations are often viewed as difficult research subjects, for many of the same reasons that information sharing infrastructure has been so slow to develop. As a research funding agency, public entity, and administrator, the DOE umbrella covers operational security programs across a great number and variety of labs, facilities, and projects. DOE has a long and established history of taking information security seriously, both in the classified and unclassified spaces. There is more than enough room in for cyber research of all kinds, but our society desperately needs a systematic understanding of real world security practice.

#### **Acknowledgements**

The author thanks Von Welch for his comments and guidance. The author thanks the the organizers of the ASCR Cybersecurity for Scientific Computing Integrity Workshop for the opportunity to submit this paper for review.