Title

The Open Science Cyber Risk Profile

Journal

IEEE Security & Privacy, 15(5)

ISSN

1540-7993

Authors

Peisert, Sean
Welch, Von

Publication Date

2017

DOI

10.1109/msp.2017.3681058

Peer reviewed

The Open Science Cyber Risk Profile:

The Rosetta Stone for Open Science and Cybersecurity

Sean Peisert | Berkeley Lab
Von Welch | Indiana University

A common misconception—one often held even by scientists—is that open science is "open" by definition, so hackers wouldn't target it. The reality is that even open science is rarely *entirely* open at all times. For example, it can often be misleading to the public or even other researchers to publish raw data before it's been verified, validated, and interpreted. Beyond situations in which raw data is published almost immediately, there are certainly many circumstances in which raw data contains valuable intellectual property that could be at risk of theft—both domestically and internationally. Or data might contain personally identifiable information, such as during clinical drug trials.

Moreover, it would be a mistake to ignore security risks outside confidentiality, including integrity and availability. While scientists might not feel anyone wants to interfere with their results, any scientist developing or testing something of commercial value can certainly be at risk of having their work tampered with in a way that causes it to behave unpredictably or to make something look more or less successful than it actually is. Consider the possibilities of tampering with science related to politically sensitive subjects or public safety, such as meteorology or public health.

The reality is that, aside from the "why me?" question, the most important issue is really the "what if" question. Producing scientific results takes months or years of careful labor of many people using expensive and often unique instruments. These results, in turn, are often built upon by others, again over months, years, or even decades. While the scientific process has done a good job of finding errors and inaccuracies in science, there are steps to help this process with regard to errors owing to computer attacks. The goal is to mitigate errors from the outset, or at least spend less time and money to identify them after they do happen.

Bringing cybersecurity to bear on open science often presents both a culture clash and a knowledge gap. Cybersecurity professionals don't have much experience with rare, even unique, scientific instruments, and the sensitivities of their data, unlike say HIPAA (Health Insurance Portability and Accountability Act) regulatory data, aren't defined. Scientists, believing themselves to not be targets, will often see cybersecurity as simply administrative hindrances to their work. The result is that the application of cybersecurity to open science can be off target—an impediment to science and less than optimally effective.

The Open Science Cyber Risk Profile (OSCRP) aims to help improve IT security for open science projects—that is, science that's unclassified and often funded by US government agencies, such as the NSF, the Department of Energy's Office of Science, and the National Institutes of Health. The OSCRP working group has created a document that motivates scientists by demonstrating how improving their security posture reduces the risks to their science, and enables them to have a conversation with IT security professionals regarding those risks so that appropriate mitigations can be discussed.

Given all the potential risks, the OSCRP working group examined a variety of different types of scientific computing–related assets and divided them into key categories, including various types of

- data (for instance, public data, embargoed data, and internal data),

Copublished by the IEEE Computer and Reliability Societies
1540-7993/17/$33.00 © 2017 IEEE

- facilities (for instance, physical storage, power, and climate control),
- system and hardware assets (for instance, networks, front ends, servers, databases, and mobile devices),
- software assets (including both internal and third-party software),
- instruments (for instance, sensors or control systems), and
- intangible and human assets (ranging from project reputation to human staff to collaborative materials and financial assets).

Note that it's key that the working group focused on *assets*, which are things that a scientist knows and cares about, rather than specific *threat actors*, which are difficult for anyone to predict and whose motivations and tactics change over time (for example, the rise of ransomware over the past few years has greatly changed the threat landscape).

To accomplish this task, we assembled a group of security experts as well as domain scientists running large science projects, including particle physicists, oceanographers, genomic researchers, and more.

This group considered a set of common open science assets as well as how open science projects relied on each—and, hence, the risks associated with each asset's failures. We then mapped possible IT threats to these science risks. Scientists can use the OSCRP document to enumerate all the assets of importance and the risks each brings to their science mission. Using this information, they can prioritize the relevant IT threats. IT security professionals can then design and implement appropriate mitigations tuned specifically for the science risks, and scientists would understand the value of these mitigations.

It's our hope that this document helps scientists better understand reasons why they might be interested in pursuing further discussions with computer security experts and, conversely, help institutional community efforts best convey important messages to domain scientists about the risks to open science.

The OSCRP can be found at trustedci.github.io/OSCRP. It reflects an initial set of assets and the group's early valuation of those assets' risks. Over time, assets will change and so will risks; hence, we envision it as a living document that will evolve over time. To this end, we followed a NIST practice and used the popular GitHub source code repository to author the OSCRP. This allows for the public's submission of proposed additions, changes, and comments on the document. Note that the lists of assets and their risks are not comprehensive; more contributions in either of these areas are welcome. We've already received some great community feedback and hope for not just more feedback but a community sense of ownership.

Although open science is indeed open, it's not exempt from the risks of computer-related attacks, and there are cultural and technical challenges to applying current cybersecurity approaches. We hope the OSCRP serves to bridge the communication gap between scientists and IT security professionals and allows for the effective management of risks to open science caused by IT security threats. ■

Sean Peisert is a staff scientist at Lawrence Berkeley National Laboratory, chief cybersecurity strategist at CENIC, and an associate adjunct professor at UC Davis. Contact him at sppeisert@lbl.gov.

Von Welch is director of the Center for Applied Cybersecurity Research and the NSF Cybersecurity Center of Excellence at Indiana University. Contact him at vwelch@iu.edu.