The Economic Impact in Biosecurity Breach – The Perspective of a Translational Scientist

Pranela Rameshwar

Rutgers, New Jersey Medical School, Dept of Medicine, 185 South Orange Avenue, Newark, NJ 07103
Email: rameshwa@njms.rutgers.edu

Received 25 January 2016; Accepted 1 February 2016;
Publication XXX

Abstract

This short opinion article discusses the overlooked problem of protecting biological data generated in biotechnology companies and at universities. This type of security should fall under the umbrella of a biosecurity and perhaps as a subgroup of cybersecurity. The article discusses some of the problems and address how the security, universities and scientists could begin to form teams to ensure the security of the data. More importantly, the article also discusses the economic impact of breach in the security data.

Keywords: Biosecurity, cybersecurity, economic impact, biotechnology, biological sciences, Pharmaceutical.

1 Introduction

Cybersecurity has been given much attention since this form of security is accepted as threats among and within sovereign nations. The interest in cybersecurity has been highlighted in the mainstream media, thereby providing a forum for the general public to realize the looming problem. In contract to cybersecurity, there is little to no attention given to the security of research data developed in biotechnology companies as well as the data in academic

Journal of Cyber Security, Vol. 5, 19–22.
doi: 10.13052/jcsm2245-1439.512

laboratories. This brief discussion proposes that such seeming disinterest in the biosecurity could have overt economic impact on businesses and by extrapolation to nations.

2 Underlying Issues

The lack the security bodies to protect research data could be due to the omission of advisors with backgrounds in the biosciences at cybersecurity forums. A more important reason for such omission might be due to the biologists/biochemists believing that their data cannot be accessed. One should also note that the focus by most scientists to be creative tend to lead to the researchers thinking about protecting the data. Thus, it is incumbent on the administrators at the institutions to ensure the security of the research data.

The medical scientists believe that compliances such as adherence to the guidelines needed to use human subjects and animals are sufficient. On the other hand, the different institutions believe if they can protect the health data from study subjects is sufficient if the files are encrypted. There are several problems with the current thoughts that could have significant impact on the economic health of scientific advances. The threats are especially important to the countries that invest in resources for their long-term growth in the field of bioengineering and other technologies such as 3-dimensional bioprinting and translational sciences with stem cells. Indeed, these intense fields have led to the design and modeling of complex process to advance medicine. Amid these successes are surprises for the investigators of the sciences. This short opinion/perspective article will not address the ethics but the biothreat posed for those engaged in the biological sciences. However, this does not mean that ethics is mutually exclusive of biothreat. The intent is to discuss how biothreat could provide a competitor with a timeline advantage to get a product to market.

3 Economic Impact

An investigator in a developed country such as the United States of America could be engaged in a highly significant study in which the outcome could have a global impact on health. A scientific group who is not affiliated to the research but is interested in the topic may not want to copy the data from the scientists who have generated a substantial amount of research information but, would be interested in the information. The purpose is to use the information to save time

so that the group could be the first to be ready for marketing. If successful, this could cost the first set of scientist significant economic loss. The cost could be widespread because intellectual property can be impacted. The question then, how can universities, biotechnology companies and pharmaceutical companies secure the data?

If the most secure information can be accessed, scientists should be aware that their data could be accessed without any knowledge that the data were accessed. Universities are not only about academic freedom but are also institution where highly developed research can lead to intellectual property for licensing and, in general, contribute to the economic 'health' of the universities. In the case where there is a breach in biosecurity, the economic impact could be wide-spread since the cost to the universities could prevent the expansion of training programs and to increase the faculty. Both types of expansions are necessary to increase the research for the development of intellectual properties. Moreover, the loss of product development would mean loss of revenue from taxes and job creation to the country.

Figure 1 is one example that could represent the consequence of biothreat to a university. The diagram shows the costly development of research at a university. The data are breached by personnel at a competitor

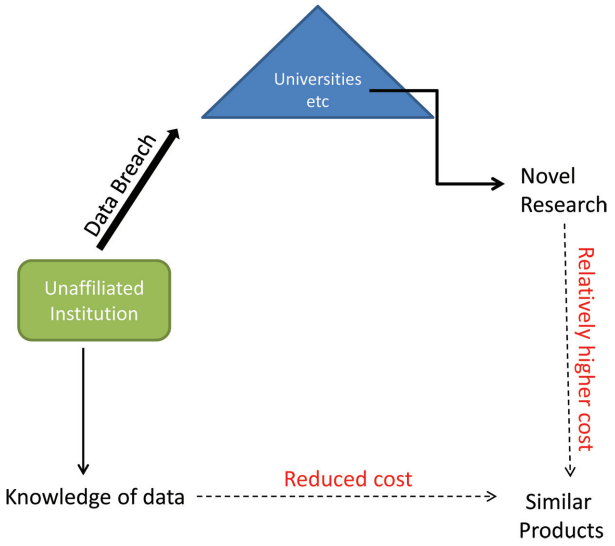

Figure 1 Consequence of biosecurity breach. Shown is a scenario in which the research data from a university is breached by a competitor company. This allowed the competitor to save on the already costly research acquired by the university. The end product by the university becomes relatively more expensive.

unaffiliated institution. The information is not acquired but is used as a method to gain information towards the same end goal. This led to the competitor developing a similar product with less cost. Due to this difference in cost, it is likely that the competitor will be in the market, causing a significant loss to the university.

In general, the above discussion only begins to discuss the issues that are probably ongoing, but not at the forefront of cybersecurity. We expect that biosecurity will continue to be a future issue in the race to develop products that boost the economies of countries. The experts in cybersecurity need to be aware that the biological sciences are a subset of information that should not be ignored. They are encouraged to engage the biologists, biochemists and bioengineers to determine how to identify and prevent biothreat.

Biography

P. Rameshwar is a professor of Medicine, Division of Hematology and Oncology at the Rutgers Biomedical Health Science, New Jersey Medical School. She received a B.S. degree in medical microbiology from the University of Wisconsin at Madison and a Ph.D. in biology from Rutgers University, New Jersey. Dr. Rameshwar performed postdoctoral studies in hematopoiesis at New Jersey Medical School. Thereafter, she became a faculty member in the same department. Her research interest is in the translation of stem cell, breast cancer dormancy with a focus on cancer stem cells. In addition, Dr. Rameshwar studies neural regulation of hematopoiesis and the immunology of adult human mesenchymal stem cells. Dr. Rameshwar has authored $>$200 publications, which include original articles, reviews, editorials and book chapters. She has also edited books.