Researchers carefully protect dangerous pathogens – but how secure are all their data?

August 14 2015, by Carole Baskin

Virus researchers know how to protect themselves and their samples. Credit: UNMEER, CC BY-ND

Ebola, smallpox, anthrax and many others: the most dangerous

microorganisms are strictly regulated in the United States. The federal government oversees use of 65 so-called select agents with "the potential to pose a severe threat to public, animal or plant health, or to animal or plant products." Before scientists can work with them to learn more, find cures or create vaccines, they must meet a long list of conditions. The goal is to keep deadly infectious agents safely under lock and key, where they can't threaten the general population or fall into the wrong hands.

But even the most physically secure research lab could be the site of a devastating data security breach. As they stand now, information security guidelines published by science regulators with regard to select agents lack the critical level of detail needed to protect data effectively.

There has never been as much research performed with these pathogens as in the past decade. The sprawl of high containment laboratories has led to a parallel increase in individuals with access to these agents. As of January 2015, approximately 11,000 individuals were on the list.

As the amount of research done on these deadly microorganisms continues to grow, the scientific community needs to wise up about information security threats and toughen up its defenses. The stakes are high. The goal is to avoid a data security breach that could, for instance, provide bioterrorists with information they could use to make already dangerous agents even more so.

Physically securing dangerous pathogens

The government has mandated strong security measures for people working with deadly microorganisms since 2001, subsequent to the anthrax events that followed 9/11.

Today, research has to be reviewed internally by a scientist's institution to assess whether safety precautions are adequate. In some cases, it's

reviewed externally as well by the National Institutes of Health (NIH) (one of the major federal sources of funding for researchers). The NIH takes particular note if potential results could be used for nefarious purposes or if recombined genetic materials are to be administered to human beings.

Personnel must pass stringent background checks. Facilities must be inspected for proper containment and physical security. Standard operating procedures must be in place to ensure protection of the agents, scientists, community and environment. All of these precautions are meant to ensure that dangerous pathogens don't infect anyone and stay safely in the lab.

Limiting open discussion

There are also policies in place that curtail how freely researchers can intentionally share information about their work on these dangerous microorganisms.

Since the implementation of the federal government's first Dual Use Research Policy in 2012, the notion that some nonclassified research information may need to be withheld has marked a big change from science's typical culture of openness. Researchers are used to running studies and experiments, then publishing details and results in freely available peer-reviewed journals.

Never before has the US scientific enterprise been as constrained as it currently is. There is even an ongoing moratorium on so-called gain-of-function experiments that involve certain agents potentially capable of causing a pandemic.

Researchers are used to sharing their science in publications and presentations. Credit: tales of a wandering youkai, CC BY

Information security at least as vulnerable

Recent safety lapses by government laboratories involving anthrax and H5N1 flu prove that despite all precautions, the system is far from perfect. And the bad news is there might be more to worry about – even if the microbes remain under lock and key and the researchers aren't deliberately sharing sensitive findings.

Vulnerabilities in information security can directly affect the physical security of dangerous pathogens. For instance, someone gaining access to a computerized key card system could use that information to enter a restricted area.

So-called "dual-use" knowledge, which could be used to weaponize some of these agents, is also at risk. In theory, a hacker could gain access to a researcher's data on how a particular microbe could become more pathogenic: for instance, by increasing its resistance to available therapeutic or prophylactic drugs.

My colleagues and I recently published an article in the journal Health Security describing these kinds of vulnerabilities. It was the result of a unique collaboration. I am an associate professor of environmental and occupational health who specializes in biosecurity. Nick Lewis came from an information security perspective. And Mark Campbell is a biosafety officer and select agent responsible official at Saint Louis University.

We found that current information security guidelines are inadequate. For instance, government agencies must abide by the Federal Information Security Management Act (FISMA), which is considered the gold standard for a risk-based approach. Unfortunately, current government-mandated information security around dangerous pathogens does not meet even the lowest standard of the act. One example: FISMA specifies how to configure a firewall in great detail; on the other hand, select agent information security guidelines mention firewalls, but don't specify how to configure or manage the firewall securely.

Why isn't research's data security cutting-edge?

Understanding of the threats unique to the academic and research environment is still evolving. There's very poor communication between the scientific community, the security community and the information technology community.

Scientists themselves are largely uneducated in matters of information security. For instance, many remain unaware that they might be targeted

to divulge sensitive information through a variety of stealth tactics. Since advances in science often depend on open communication and sharing data, scientists aren't trained to be wary of inquiries about their work.

Many also don't recognize that shared computer systems and laboratory equipment capable of storing or transmitting data – from microscopes with digital photography capability to freezers that send emails when temperatures are too high – are sources of vulnerabilities. After all, everything connected to a computer network is at risk, even if it doesn't look like a computer.

How to lock down the information, too

First (and obviously), the standards required for government agencies by FISMA should be implemented for information related to research with dangerous pathogens. This is a matter of carrying out what the law already calls for.

Secondly, there should be a secure way for research institutions to exchange information about current information security threats, as well as effective strategies to protect scientific data that could be misused. While implementing these measures now is not without monetary and time costs, they would prevent the big security and research expenses that would be incurred after a major security breach and implementation of reactive measures.

Finally, there should be more concrete efforts at effective communication between science, information technology, and security experts, so they may understand each other's disciplines better. An effective approach could include educational opportunities for individuals who are interested in working at the interface of these very different communities.

My colleagues and I found writing our research paper to be difficult because we were all outside of our comfort zones. Professionals, whether they are life scientists or computer people, do not like to admit that they don't know or understand something. When we had to ask each other for explanations regarding simple concepts in the others' fields, it was humbling.

But we have proved it can be done. The cross-disciplinary conversations must continue. Information security concerns are not going away, so we need to awaken to this reality before a major disaster happens.

Source: The Conversation