ICE

TRUSTED IT PARTNER

ICE's Ultimate Guide to

EFFECTIVE CYBERSECURITY: LIFE SCIENCE LAB SECURITY

Solutions to Security Challenges for Life Science Labs

ICE
TRUSTED IT PARTNER

As a managed IT and cybersecurity provider for Life Sciences we unfortunately are witnessing firsthand the carnage cybercrime is having on this industry. We have seen this trend unfolding for quite some time. However, in the past few months there has been an unprecedented level of ransomware attacks in biotech. One of the most vulnerable points of attack we are seeing breaches is Life Science Labs.

> “Scholarly research is a target” because of its innovative nature and commercial value, says Daniel Ayala, chief security and trust officer for Dotmatics Group, a scientific informatics company.
>
> The life science space has largely ignored security threats for a long time. As a result, “We're are atrociously ill equipped, and we need to change that,” according to Charles Fracchia, co-founder, **Bioeconomy Information Sharing and Analysis Center** (BIO-ISAC. “We’ve been in a really bad situation for a while and have now passed a real inflection point.”

Key life science cybersecurity challenges

The largest security concern for managers of life sciences labs is a general lack of focus on security. The entire scientific process is powered by digital tools, individuals should be digital experts. Although cyber hygiene is not taught to scientists, in the coming years it will be impossible to succeed without understanding some basic cybersecurity principles.

Lab Security should consist of data availability, integrity, and confidentiality. Integrity is a factor that is taking on more and more significance. Lab administrators must make sure that the data is accurate both when it is captured and throughout its full life cycle.

The greatest threat to lab managers is espionage, therefore they should focus more on protecting the data rather than caring about operations and availability.

3 WAYS TO INCREASE YOUR LABS SECURITY

1

Protect your labs data

Identifying the problems, you're seeking to tackle is the first step. Then, decide which best practices are most appropriate for your industry and environment.

Adopting a post-breach perspective is maybe the most crucial step. Consider the possibility that your network has been compromised, giving someone else access to all your data. It is crucial to establish an Incident Response Plan. Select the teams, materials, and communication channels you'll need to quickly put together for a forensics investigation that will show when, and how the intrusion happened and what was impacted. Maintain a paper copy of the plan of action as well, as ransomware attacks can shut out computers.

Even if you aren't thinking about a breach, be cautious whenever something seems odd. If data seems unusual, horrendously terrible, or if the instruments start acting suspiciously, trust your gut. Investigate the problem. Doing an antivirus check is a good first step in confirming that the data hasn't been altered.

2

Protect your lab network and instruments

Laboratory instruments and equipment is another issue. The level of security afforded to lab equipment is lower than that of other electronic assets. Hence, a ransomware assault could cause labs to lose all their research data or to be retrained to report results incorrectly, take data for analysis from the incorrect cells, or experience other types of security breaches.

Strong passwords and multifactor authentication are the first line of defense in protecting such equipment as well as the lab's network. As soon as security patches and other software or firmware upgrades are made available for instruments, install them. Check the instrument's settings to make sure that the possibility for automatic software and firmware updates is enabled.

Keep copies of lab data all the way back to its origin. Then, to ensure the path can be followed, he advises backing up data by keeping three copies of the data, using two different storage mediums or systems, and keeping one copy offsite (such as in the cloud).

While making commitments for the delivery of research, lab managers should factor in time for security and maintenance for each project. Security is part of the upkeep.

3

Remote Access Protocols

Examine remote access carefully to lower the chance of a hacker penetrating your lab. There is a significant danger involved in permitting users to use their personal devices (laptops, tablets, and phones) to access the laboratory network, its tools, and equipment.

During the pandemic, remoting-in to check on experiments became a normal way for scientists to work while reducing their presence in their labs, Yet, allowing users to access the laboratory network and its instruments and equipment from their personal devices (laptop, tablet, phone) poses a huge risk. These devices are susceptible to phishing scams and malware that can infect them and spread to the organization's networks. Once inside, malware can shut down activities or steal and corrupt data. It might end up costing the company millions of dollars.

To lower the dangers, the computing resources in the lab should be isolated from the organization's network and made more difficult to access. That involves working with IT to install firewalls, and using local drives and performing analyses on dedicated, air-gapped computers. The most important thing they can do is to physically break the network connection between the machines of individual users and the lab network.

A complete air-gapping of the lab is often not practical. Using cloud-enabled solutions lessens the inconvenience by facilitating easy access to data while yet maintaining the lab's integrity. Nonetheless, the lab network itself as well as cloud computing possibilities should continue to demand strong password systems and two-factor authentication.

THIS SITUATION IS ONLY GETTING WORSE

The increase in data breaches began to escalate with the COVID Pandemic. Unfortunately, unlike COVID the CYBER Pandemic is just getting started.

- Life Science organizations will lose over 647 billion dollars to cyber attacks in the next few years – Accenture.
- Ransomware attacks on healthcare organizations were predicted to quadruple from 2017 to 2021 and 2022, and they are expected to continue trending up – Cybercrime Magazine.
- Ransomware attacks against healthcare organizations doubled in the last five years, with the most common victim being health clinics, according to a new JAMA Health Forum study.
- Pharmaceutical companies are now routinely targeted and attacked by these advanced threat actors, and in 2021 almost all (98%) of pharmaceutical companies experienced at least one security intrusion.

These 3 steps are just a start. Lab managers alone should not bear the full burden of protecting their labs. It is important they form a strong relationship with your organization's IT and cybersecurity teams. Working together will allow your IT team to implement security that protects your labs but also supports lab manager's goals.

ICE Consulting has been an IT and cybersecurity provider for the Life Science community for over 25 years. We have helped countless biotech companies design, build, and most importantly secure their lab networks, systems, and stations.

CONTACT US TODAY FOR A FREE SECURITY POSTURE LAB ASSESSMENT

888-423-4801
www.iceconsulting.com