ICE
TRUSTED IT PARTNER

ICE INDUSTRY REPORTS:

HOW CYBERSECURITY IS IMPACTING BIOTECH FUNDING

ICE INDUSTRY REPORTS:

HOW CYBERSECURITY IS IMPACTING BIOTECH FUNDING

The life sciences industry has become one of the top targets for cyberattacks. At the 2023 RSA Conference, Lisa Monaco revealed that biotech has surpassed finance and joined healthcare as the #1 industry under threat from hackers. Accenture estimates that life sciences organizations will face a staggering $647 billion in losses over the next four years due to cybercrime.

Despite being clear targets, many startups in this field neglect cybersecurity. The most common excuse? "We're too small." Startups often operate with minimal IT infrastructure—just a few laptops and some cloud-based applications—leading them to believe there's nothing worth protecting. This mindset, however, is a critical mistake.

Firstly, IBM's "Cost of a Data Breach" report found that 43% of data breaches last year targeted SMBs and startups. Hackers know small companies rarely invest in robust cybersecurity, making them easy prey. Secondly, the same report revealed that 82% of data breaches involved public cloud applications. This "too small to target" assumption has created a golden opportunity for hackers.

Even if your company doesn't have much to lose today, hackers can exploit unprotected systems, gaining access to endpoints and lying dormant for months—or even years. When news breaks of your startup landing a grant or securing funding, they're ready. Using the backdoor they created, they strike just as your business begins storing valuable data. The result? A ransom note demanding payment, now that they know you have the funds.

This growing threat is not going unnoticed. Funding agencies are increasingly prioritizing cybersecurity when evaluating grant applications. Proposals lacking robust cybersecurity measures are often deemed too high-risk, leading to rejections. In short, a lack of investment in cybersecurity doesn't just endanger your data—it could jeopardize your chances of securing critical funding.

For startups in the life sciences, cybersecurity is no longer optional. It's a fundamental requirement for growth, protection, and long-term success.

KEY REASONS WHY GRANT APPLICATIONS MIGHT BE REJECTED DUE TO WEAK CYBERSECURITY:

Insufficient risk assessment:

Not conducting a thorough analysis of potential cyber threats and vulnerabilities within the project scope.

Poor data protection practices:

Lack of encryption for sensitive data, inadequate access controls, or weak password management.

Inadequate incident response plan:

Not having a well-defined plan for responding to and mitigating cyber incidents.

Lack of employee training:

Not providing sufficient cybersecurity awareness training to staff, which can lead to human error vulnerabilities.

Outdated security systems:

Relying on outdated technology or software that lacks essential security features.

Non-compliance with industry standards:

Failing to adhere to relevant cybersecurity frameworks like NIST or HIPAA depending on the project area.

Lack of an IT Infrastructure:

Even if your IT infrastructure consists of a few endpoints and a handful of cloud applications you should still have a secure cloud infrastructure capable of growth.

WHAT GRANT APPLICANTS CAN DO TO IMPROVE THEIR CYBERSECURITY POSTURE:

Comprehensive risk assessment:

Conduct a detailed evaluation of potential cyber threats and vulnerabilities specific to the project.

Implement strong security controls:

Deploy robust measures like firewalls, intrusion detection systems, data encryption, and access controls.

Develop incident response plan:

Create a well-defined plan for handling cyber incidents, including data breach response strategies.

Employee cybersecurity training:

Provide regular training to staff on cybersecurity best practices, phishing awareness, and password hygiene.

Third-party vendor management:

Assess the cybersecurity posture of any third-party vendors involved in the project.

Clearly articulate cybersecurity strategy:

In the grant application, explicitly outline the cybersecurity measures that will be implemented to protect project data.

Implement an IT Foundation regardless of size:

Implement or outline a cloud based IT infrastructure that protects your endpoints and cloud applications according to best practices.

THE BLUEPRINT

Avoiding security pitfalls requires a little time and a clear understanding of the necessary security controls. At ICE Consulting, we bring over 25 years of expertise in IT and cybersecurity solutions tailored to biotech startups. Our mission isn't just about delivering services to the life sciences community—it's about empowering them with the tools and knowledge to confidently navigate their path to commercialization.

In our guide, "Protecting Your Biotech Startup," we outline an actionable blueprint designed specifically for startups with minimal infrastructure—think a few laptops, a couple of cloud applications, and remote employees. This cloud-based solution provides a comprehensive suite of security features at an affordable cost of just $20 per user per month. Even better, for teams with only a handful of users, the initial setup is significantly more cost-effective than waiting until your team grows to dozens. Once configured, your system can seamlessly scale as your team expands, eliminating the need for repeated setup.

This security design achieves three critical objectives: stability, scalability, and cost-efficiency—empowering biotech startups to focus on innovation without compromising on security.

#1

Guarantees your security posture supports, rather than hinders, your chances of securing funding.

#2

Protect your data, communications, and intellectual property.

#3

Establish a scalable cloud foundation to support your growth when funding comes through.

CALL OR EMAIL TO GET YOUR BLUEPRINT TODAY

ICE
TRUSTED IT PARTNER

☎ 888-423-4801
✉ info@iceconsulting.com