ICE
TRUSTED IT PARTNER

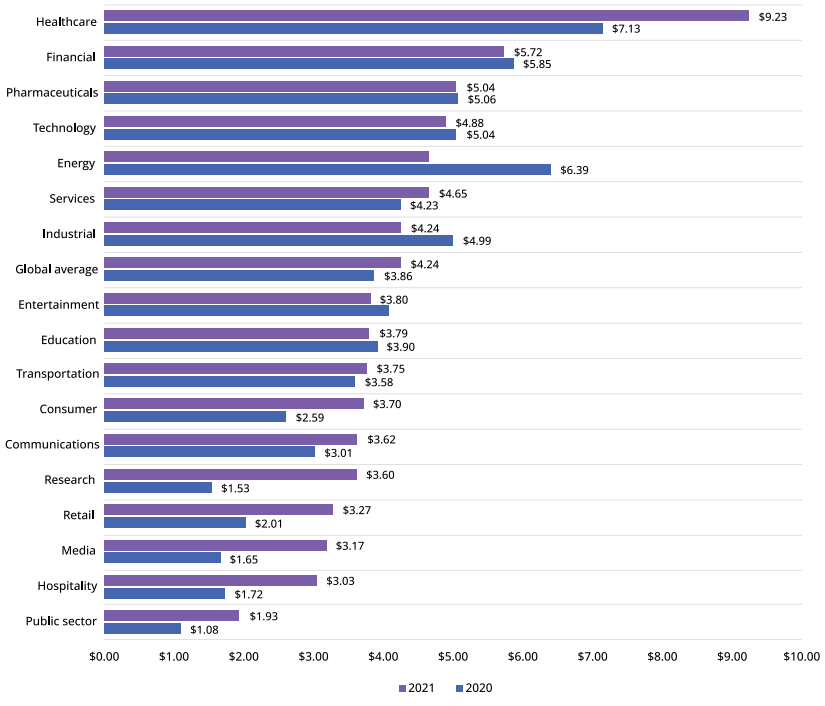
SOC OPERATIONS

The cost of protecting your Biotech startup on your way to commercialization

It is no secret that data breaches are escalating year after year with a 5-fold increase in 2020 alone. The Healthcare industry has been the #1 target for 11 years in a row with the Pharmaceutical and Technology sectors coming in at #3 and #4.

Average total cost of a data breach by industry

Measured in US$ millions



Healthcare was the top industry in average total cost for the eleventh year in a row.

The top five industries for average total cost were:

1. **Healthcare**
2. Financial
3. **Pharmaceuticals**
4. **Technology**
5. Energy

The average total cost for healthcare increased from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Energy dropped from the second most costly industry to fifth place, decreasing in cost from $6.39 million in 2020 to $4.65 million in 2021 (27.2% decrease).

Other industries that saw large cost increases included services (7.8% increase), communications (20.3% increase), consumer (42.9% increase), retail (62.7% increase), media (92.1% increase), hospitality (76.2% increase), and public sector (78.7% increase).

YOUR REACTIVE STRATEGY COULD SPELL DISASTER

Do your thoughts on cybersecurity fall into one of these categories?

The box checker: "We need to be compliant, that's all that matters."
The blissfully ignorant: "We'll worry about cybersecurity later."
The responder: "We only protect against problems we have had in the past."

These are just a couple of examples of the excuses we hear every day. If you fall into this category let me, ask you…

> *Do you think it would be a good idea to wait until your house burned down to invest in fire insurance?*

Of course not, that could cost your family everything, right? Well, if you look at the latest figures from the Ponemon Institute and IBM you will see the damages from a data breach could cost your company everything:

- The average total cost of a data breach is now 4.24 million dollars
- For companies with less than 500 employees are still looking at an average total cost of 2.94 million dollars
- There is now a $180 fine for every compromised record containing a Customers' Personally Identifiable Information (PII)

The costs of the breach alone are immense, and that is not even factoring in the potential loss of IP, or compromised research, damage to your brand and reputation, and countless hours in lost productivity.

The reality is that 60% of businesses are now closing their doors after a cyber attack. Now the chances of your house catching on fire may be slim, but over 80% of firms in 2021 reported some form of an attack on their system. So, it is not a matter of if, but when and will you be ready.

EVERY BIOTECH COMPANY SHOULD DEPLOY A 24X7X365 PROACTIVE STRATEGY

You Cybersecurity strategy should include the following:

Anti-Virus / Anti-Malware / EDR	**Firewalls with UTM** URL & DNS Filtering Threat Detection / Threat Prevention IDS / IPS	**Single Sign On / Multi Factor Authentication**	**Data encryption**
Behavioral analytics	**Threat hunting**	**Email filter tuning and quarantine management**	**Servers & storage in data centers**
Firewall/WAF, Servers on cloud infrastructure	**Log aggregation**	**Identity Access Management (IAM)**	**Hosted Email services**
Penetration Testing	**Wireless rogue activity detection**	**Monitoring of critical data flows**	**Threat intelligence feed analysis**

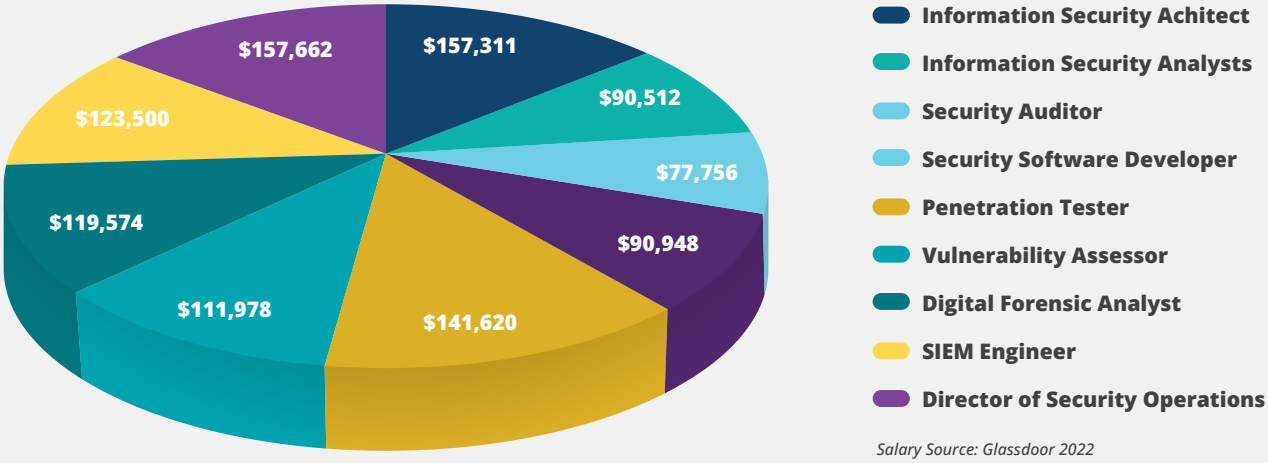
To properly perform these duties organizations need security specialists. Most IT generalists do not have the experience or knowledge to properly conduct these security practices. A proper Security Operation Center should consist of the following:

- Information Security Architect
- Information Security Consultants Specialist
- Information Security Analysts
- Security Auditor
- Security Software Developer
- Penetration Tester
- Vulnerability Assessor
- Digital Forensic Analyst
- SIEM Engineer
- Director of Security Operations

Developing this department internally requires both a significant CAPEX and OPEX investment.

STANDARD BIOTECH SECURITY OPERATION CENTER

Annual Salaries



Salary Source: Glassdoor 2022

Running an internal SOC department is a $2,000,000 a year operation

A Security Operation Center is a 24x7x365 department, meaning several of these positions require at least 2-3 employees to cover nights, weekends, and holidays. Once you add overtime, taxes, and benefits you are looking at well over $2,000,000 dollars a year to properly staff your Security Operation Center.

FINDING AND KEEPING THE RIGHT TALENT

The number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021, from 1 million to 3.5 million, according to Cybersecurity Ventures. Even if you have the $2M in your budget to pay the salaries and costs to build your SOC team, finding the right talent and most importantly keeping them on board is in itself a real challenge.

THE SOLUTION:

ICE'S SOC-AS-A-SERVICE

For a fraction of the cost, you get assigned your own personal Security Operation Center, with a team of expert engineers, monitoring your organization 24x7x365, using the cutting-edge SIEM with AI technology from Securonix.

Contact us today for a FREE DEMO on how to protect your organization. When it comes to data breaches it is not a matter of "if" but "when." ICE will make sure "when" they try your organization will be ready and waiting!