Protect Your Business with the Right Cybersecurity Investment

By now, companies know that cybersecurity needs to be a top priority. It is no longer a matter of "if," but "when" a company will experience a cyberattack. Whether an organization is specifically targeted or it's simply an act of opportunity, cyberattack risks are a part of doing business today. If left unchecked or poorly mitigated, security vulnerabilities can have huge ramifications for organizations.

IBM's Cost of a Data Breach 2021 report[(1)] found that it takes organizations an average of 287 days to identify and contain a data breach, at an average total cost of $4.24 million. A large portion of that cost results from lost business due to the breach. Even organizations that think they are prepared might have missed something, as an attack can come from just about anywhere. Various circumstances can lead to a data breach, ranging from malicious attacks (52%) to cloud misconfigurations (19%) to even employee error (23%)[(2)]

As cyber risk becomes increasingly more complex, it is then all the more challenging to adequately address the issue. Not only do organizations contend with an ever-evolving risk landscape, they are also faced with a cybersecurity talent shortage. Projections pointed to 3.1 million unfilled cybersecurity roles globally by 2021 [(3)] and CyberSeek shows more than 500,000 open positions in the United States [(4)]. This leaves some major gaps that companies may have trouble filling. For organizations that cannot acquire the in-house talent, or simply want access to a robust team fully dedicated to security, Security as a Service (SECaaS) is an increasingly popular solution.

Benefits of Security as a Service (SECaaS)

SECaaS makes it easier for organizations of any size to address and keep up with a range of cybersecurity needs. SECaaS can be used for specialized security tasks or can take the brunt of security heavy lifting off your plate. Overall, outsourcing security via SECaaS has a variety of business benefits.

> *"In 2019, spending in the cybersecurity industry reached around 40.8 billion U.S. dollars, with forecasts suggesting that the market will eclipse 54 billion U.S. dollars by 2021 as the best-case scenario, taking into account the coronavirus (COVID-19) impact."*

Cybersecurity Expertise

When you partner with a SECaaS solution provider, your security is their primary focus. This means you benefit from extensive expertise without the need to build out or overtask in-house teams. These organizations are staffed by cybersecurity experts, giving you access to some of the brightest minds in security.

Breadth of Talent

Cybersecurity is not a single-faceted practice. Different security professionals specialize in different areas. For example, an infrastructure security expert may not be well versed in cloud security. It would cost an astronomical amount of money to keep a wide breadth of cybersecurity talent on staff and to hire new talent as new technology areas emerge. Without SECaaS solutions, the alternative is to unknowingly have security gaps or hope your in-house team does a “good enough” job to protect your business. In security, there is no “good enough.” The risk of irreparable damage is too high. SECaaS gives you easy access to all the talent you need across specialty areas.

Keeping Up with Change

Unfortunately, cybersecurity attacks and vulnerabilities are on the rise and require constant vigilance. When you work with a SECaaS provider, they are solely focused on security and have the expertise to monitor the risk landscape as well as your specific vulnerabilities to quickly adapt to changes. This makes it easier for you to protect your business.

Predictable Cost

One of the benefits of SECaaS solutions is cost predictability. In-house staff require salary negotiations, raises, bonuses, benefits and other expenditures. Hiring new staff or replacing personnel also comes at an additional charge. When you contract with a SECaaS provider, you will be notified of all monthly or yearly costs upfront so that you can prepare for a provider that best fits your needs.

Best Practices for SECaaS

While SECaaS has many benefits, there are still best practices you should follow to ensure you get the most out of your relationship. Understanding these parameters will also help you ensure you are getting what you expect from your SECaaS partnership.

Understand What’s Covered

Some SECaaS providers offer more extensive solutions than others. Whether you use a comprehensive provider or a specialty service, you should have a full understanding of what is — and isn’t — covered by their services. Security issues can arise from being under the wrongful impression that your SECaaS provider monitors an aspect of security that they do not.

Some providers may directly address issues while others will only identify vulnerabilities then hand over for your in-house team to resolve. Choose a provider that best matches your needs. If your in-house team is not equipped to address a wide variety of issues, seek a provider that will handle risk mitigation and issue resolutions for you. In either case, have a clear understanding of the provider’s incident response times to ensure it meets your internal requirements.

If you're outsourcing all aspects of your cybersecurity, you may need to use multiple providers. Understand what services each offers and build the solution portfolio that's right for your organization and covers all major vulnerability areas.

Discuss Compliance

Many compliance standards have specific security components. Working with a SECaaS provider can help you meet those requirements, making it easier to achieve and prove compliance. Ensuring your SECaaS provider's services are compliant may even be a specific requirement for your business.

If you're in a compliance-heavy industry, do not assume any SECaaS provider you work with will be able to meet those standards. Ask specific questions and request to see documentation.

Establish Responsibilities

It's important to understand what cybersecurity services the SECaaS provider will cover and what responsibilities you have. This will help prevent security gaps from lack of communication. It's also important to understand responsibilities for compliance purposes. No SECaaS provider can meet 100% of your compliance requirements. The service provider will be responsible for some, some will be shared, and some responsibilities will remain with you. If you're working with a SECaaS provider to meet compliance standards, ask for a detailed RACI and keep a copy for your records.

Ask About Industry Experience

While some cybersecurity risks are universal, some industries may experience specific risks. If you're in a high-risk or compliance-heavy industry, such as healthcare or financial services, seek a SECaaS provider that specializes or has experience in your industry.

For Additional Information Please Contact
Laura Baustian
SIS Holdings Group, LLC
E: lbaustian@sis-holdings.com

Finding the Right SECaaS Provider

Cybersecurity is a complex undertaking and partnering with a SECaaS provider can help you address areas you may struggle with and fill gaps on your team. For smaller organizations, a SECaaS provider may even become your main cybersecurity protection. With correct vetting and an understanding of what each provider offers, a SECaaS provider can be the right investment to protect your business.

---

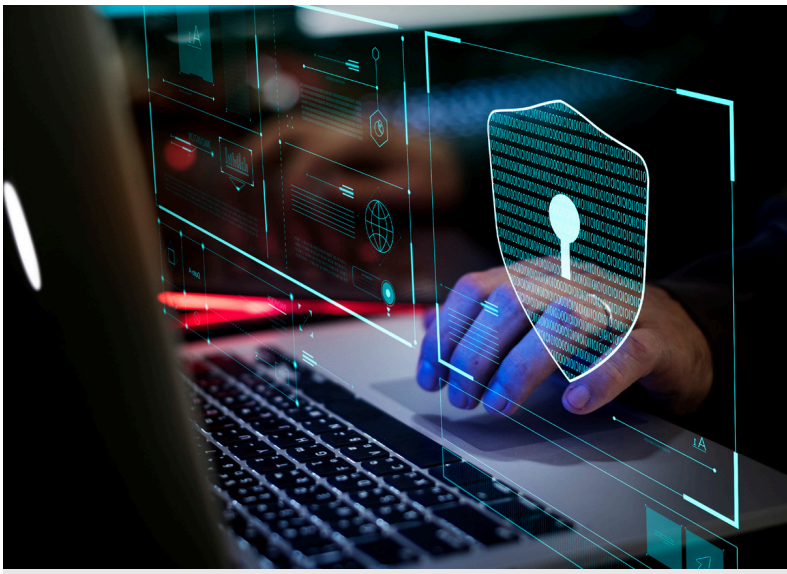
(1) IBM, "Cost of a Data Breach 2021," 2021.
https://www.ibm.com/security/data-breach

(2) IBM, "2020 Cost of a Data Breach Report," 2020.
https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

(3) Cybersecurity Ventures, "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021," October 24, 2019.
https://cyber securityventures.com/jobs/

(4) CyberSeek, 2020.
https://www.cyberseek.org/heatmap.html

(5) Canalys,"Global Cybersecurity 2021 Forecast." January 2021.
https://www.canalys.com/newsroom/canalys-cybersecurity-2021-



Sound interesting? Let's talk.

Contact us today to get started!