

The Decision-Maker's Guide to Combating Cyber Threats

How to advance your IT strategy to meet the demands of an increasing cyber threat environment

It's no secret that cyber and security events have rapidly increased in recent years. By September of 2021, the number of reported security incidents suffered in the U.S. had already surpassed the number of incidents in 2020, which itself was a record year.

These rapid transformations and the sudden influx of new technologies have ignited a new era of business—one where your IT architecture and security strategy matter more than ever, and industry competition is a battle between companies who are the most secure and stable, on top of providing the best service.

So how do you invest your money and resources wisely to stay on top of the ever-evolving threat landscape?

The rise of data breach and ransomware incidents

Data breaches and ransomware cyberattacks have evolved from rare occurrences into a thriving market. In fact, damages incurred from reported security incidents exceeded \$6 trillion in 2021 (doubling from \$3 trillion in 2015).



In contrast to the early 21st century when the threat landscape saw drastic changes in the types of cyberattacks occurring in the time frame of a few years, data breaches and ransomware have shown to evolve much more quickly in recent years. Experts expect the number of ransomware attacks to increase and newer forms to become more sophisticated and disruptive in coming years.

Today's cyberattacks can take the shape of ransomware, denial of service attacks, phishing, cross-site scripting, DNS tunneling, credential breaches, and more.

What does this sudden increase in both type and number of cyberattacks mean for you?

Implement cybersecurity safeguards as a foundation of your IT strategy, not an add-on

In bygone eras, companies could make do with an optional antivirus add-on to their IT tech stacks to protect their day-to-day business operations. But with cyber criminals extorting new system vulnerabilities every single day—from the rise of bots to for-profit malware and high-profile systemic attacks—a strong cybersecurity framework is no longer optional.

Cyberattacks are costly to mitigate, especially if they shut down production, require new systems, or cause a loss of company data, intellectual property, or customer personal information. And unless your day job is cybersecurity, it's nearly impossible to keep up with so many types of threats and the necessary measures to put in place to safeguard your company from different types of attacks.

But how can investing in a robust cybersecurity framework add to your bottom line?

Only 35% of **SMBs** could **remain profitable** for more than three months if they lost access to essential data, with **more than half** becoming unprofitable in under a month.

A \$100 billion enterprise that experiences a typical cyber event should expect a cost that represents less than 1% of annual revenues.



A SMB that brings in **\$100,000** per year, on the other hand, will likely **lose**

25% of its earnings or more.

IBM

The business case for investing in a strong cybersecurity framework

As a decision-maker, we know that most of your decisions come down to ROI. There is no doubt that cybersecurity and new IT solutions represent a financial investment. But any security investment should be considered against its contribution to the protection of a company's most important asset - its data.

When properly orchestrated, a strong cybersecurity foundation can add to your bottom line by:

- Minimizing operational, financial, and regulatory business impacts of cyber threats
- Lessening the remediation costs of cyber incidents by reducing incident volume and quickly containing incident sprawl
- Providing a differentiator to gain customers and contracts and increase value of your services
- Accruing new revenue sources by adding security capabilities (for example, monitoring and response) into an existing product suite of services

While the business case for adding a strong cybersecurity framework has evident benefits, you want to invest wisely. One of the easiest ways to build a strong cybersecurity framework is by partnering with a Managed Service Provider (MSP) or Managed Security Services Provider (MSSP) to guide you through the implementation process. But not all MSPs/MSSPs are created equal.

An integrated approach to IT and cybersecurity

Most other IT service providers offer cybersecurity services through a third-party partner. Without the “full picture” of your entire IT environment accessible in-house, that third-party provider can respond to a security incident, but cannot contain it—much less minimize the vulnerabilities that led to the incident itself.

When looking to invest in a strong cybersecurity foundation as part of your IT strategy, you want to look for a provider who brings an integrated approach to IT and cybersecurity. With a cohesive IT and cybersecurity strategy from one unified service provider, your company receives a higher standard of protection and is able to leverage technology to gain a competitive advantage.

Corsica SecureSM combines one integrated in-house team to not just respond to threats, but to proactively prevent and contain threats while helping your company to achieve a more productive and secure IT tech stack. By understanding the ins and outs of your entire IT environment, Corsica Technologies works with you to build a secure, efficient domain to support your business initiatives now and set you up for growth in the future.

As cyber threats evolve, so do your IT “business basics”

With an ever-changing threat landscape, integrating cybersecurity into your IT strategy is an essential building block of productive, growing companies.

To learn your next steps to defending your organization against the daily evolution of cyber threats and integrating your daily IT foundation for security and growth, schedule your complimentary risk assessment.

[Get your free assessment](#)

About Corsica Technologies

Consistently recognized as one of the country’s top managed IT and cybersecurity providers, Corsica Technologies helps organizations leverage technology as a competitive business advantage. Our integrated IT and cybersecurity services protect companies and enable them to succeed.

**Accelerating Your
Business Success.**

sales@corsicatech.com (855) 411-3387 corsicatech.com

corsica
technologies