Cybersecurity strategy is the most important security strategy.

A **cybersecurity strategy** is comprised of high-level plans for how an organization will go about securing its assets and minimizing cyber risk. Much like a cybersecurity policy, the cybersecurity strategy should be a living, breathing document adaptable to the current threat landscape and ever-evolving business climate. Typically, cybersecurity strategies are developed with a three-to-five-year vision but should be updated and revisited as frequently as possible.

While cybersecurity policies are more detailed and specific, cybersecurity strategies are more of a blueprint for your organization to guide the key stakeholders as the company and business environment evolve.

Goals for your cyber strategy

One of the most critical goals for any cybersecurity strategy is *achieving cyber resiliency*. To be resilient, business leaders must remember that each organization is unique and requires a customized approach to strategy. Much like relying upon one security product or vendor to completely eradicate all threats, there is no single cybersecurity strategy that adequately addresses every business's needs.

To achieve the ultimate goal of resilience, your cybersecurity strategy will require a mindset

shift from reactive to proactive. Instead of focusing on reacting to incidents, the most effective strategies stress the importance of preventing cyber-attacks. That said, any robust cybersecurity strategy also puts you in a better position to respond to an attack. In the event your organization is victimized, a successful strategy can make the difference between a minor incident and a major one.

Benefits of proactive cybersecurity

When it comes to managing risk, a proactive approach is always superior to a reactive one. But being proactive, especially when new threats are discovered and detected at such an alarming rate, is easier said than done.

Unfortunately for most organizations and cybersecurity departments, taking a reactive approach is the norm.

proactive cybersecurity approach not only puts you ahead of attackers but can help you maintain and even exceed regulatory requirements. Proactive strategies offer the structure and guidance that help you stay prepared and avoid confusion that may arise. With uncertainty and confusion minimized, measures for incident prevention, detection and response are dramatically improved.

When you embrace proactive security, your organization will be positioned to:

- Ensure that cybersecurity aligns with your business vision
- Foster a security-conscious culture
- Understand your high-risk areas
- Implement an assessment program to identify risks, threats, and vulnerabilities
- Approach security beyond compliance

- Invest equally in prevention, detection, and response

Developing a cyber strategy for your business

Running your business without a cybersecurity strategy is like playing a game of whack-a-mole: as soon as one incident is squashed, another pops up.

Building a cybersecurity strategy is equally

challenging: you need to address resource shortages, manage a complex technology stack, train end-users, manage expectations of the board, and strive for compliance. On top of that, all the pieces of the strategy must be cohesive; tools and resources that aren't in sync can restrict visibility into the changing events and risks across an organization's security landscape. Plus, a non-integrated system creates a high risk for human error, and checking data across multiple consoles is incredibly time-consuming.

Successful companies must transform their security programs to better align with their business and IT strategies. Effective security strategies require a risk-based approach that balances people, processes, and technologies.

First, think beyond a single solution

When thinking about your vision, strategy, and roadmap, make sure you understand the

difference between each of these themes.

Your security strategy should provide the guidance necessary for your organization to address the requirements above so that risk can be mitigated to an acceptable level by implementing general IT controls, minimizing exposures, and other means. The security strategy should allow for proper budgeting for security initiatives and a defendable prioritization model to implement these initiatives.

Cyber frameworks and templates to consider

While all this strategy planning and paving the road to resiliency might sound overwhelming, there are several frameworks to get you on the right path.