# Bridging the Cybersecurity Skills Gap Safeguards Critical Assets

In 2019, major news outlets reported the prediction that 3.5 million cybersecurity jobs would be left unfilled by 2021. And then the pandemic hit, throwing another wrench in the rapidly evolving threat landscape. To protect vital data assets, companies need to act quickly and decisively to address the cybersecurity skills gap within their organizations.

As 2021 moves into the second quarter, we see that prediction being fulfilled. While the skills gap brings career opportunities for trained security professionals, it spells danger for organizations across the globe. Without effective cybersecurity, companies put critical data and processes at risk.

## Contributing Factors that Widened the Cybersecurity Skills Gap

In recent years, a few key situations have contributed to the cybersecurity skills gap:

- **Move from on-premises systems to cloud** – Ten or fifteen years ago, organizations stored their data on premises in a handful of environments. Managing and securing those environments proved relatively simple. Mass cloud migration and the proliferation of hybrid environments has resulted in a much more complex system to secure.

- **COVID pandemic** – The 2020 pandemic introduced unexpected twists. Entire workforces switched to remote work practically overnight, broadening the attack surface and exposing vulnerabilities. At the same time, the pandemic interrupted the revenue stream, leaving IT funding uncertain.

- **Cybercrime epidemic** – As the global health crisis took center stage, cybercrime has also grown to epidemic proportions. Some experts estimate a cyberattack increase of 63 percent in relation to the pandemic as criminals have taken advantage of changing work environments and exploited fears.
- **Privacy regulations** – GDPR went into effect in May 2018, followed by a wave of additional privacy laws that mandate heightened data security. Regulatory compliance adds new wrinkles to an already-complex cybersecurity environment.

## Broaden Cybersecurity Knowledge in Organization

While cybersecurity professionals remain in high demand, data security has become everyone's business. To begin with, every IT professional within the organization needs to understand cybersecurity. IT can no longer afford to operate in siloes, with security limited to a few specialists.

In addition, employees throughout the organization must understand their role in protecting the company's data assets. Anyone with access to digital systems presents a risk. Consequently, organizations must place high priority on cybersecurity training to help employees learn best practices for recognizing and mitigating cyber risks.

## Benefit from Automation

Automation can help, particularly with organizations that lack sufficient skilled security professionals. Security solutions that use artificial intelligence and machine learning, for instance, can proactively address cyberattacks before damage occurs. Keep in mind, however, that these solutions require proper management, or they may actually introduce vulnerabilities.

## Buy-in from Executive Team

Effective cybersecurity strategies require executive support. Protecting organizational data assets involves implementing the right tools and hiring the right people. When the executive team and the security team work closely together, security initiatives line up with business goals, and everyone wins.

## Partner with Cybersecurity Professionals

For organizations that struggle to find and retain the personnel they need, enlisting the help of cybersecurity professionals can fill the security gap. Starting with a thorough security assessment, they will address vulnerabilities that put your company at risk. Then they will help you design and implement a comprehensive security strategy and provide 24/7/365 monitoring.

The security experts at Messaging Architects offer a host of services designed to protect your data. For example, they can provide email encryption, dark web scanning, data loss prevention and compliance monitoring. In addition, they can help you update your internal security policies and implement essential business continuity planning.