

# Identifying Gaps in Your Cybersecurity

**In the digital age, you cannot afford to leave your business unprotected. Cybersecurity is of paramount importance. Think your organization is too small to be the victim of a cybercrime?**

**Think again.**

Research has shown that small and medium-sized businesses are becoming increasingly likely targets for hackers. Even small organizations often hold valuable personal information such as birthdays, payment information, and passwords that cybercriminals can sell on the black market.

This is why it is so essential for you to understand where you stand when it comes to your security posture. How strong are your passwords? Is your software patched and up-to-date? Do your employees know how to tell the difference between a phishing email and a genuine message?

If you can't answer these questions, your organization is probably already vulnerable to an attack.

## **You can't protect what you don't know**

The first step in identifying gaps in your cybersecurity is conducting a comprehensive risk assessment. This should include an analysis of current systems, processes, and policies, as well as any potential vulnerabilities that attackers could exploit.

Risk assessments should also consider external factors such as third-party vendors or partners who may have access to sensitive data or systems.

Understanding the full scope of risks associated with an organization's digital infrastructure makes it easier to identify areas where additional security measures may be necessary.

**We meet you  
where you are  
and walk you  
through your  
assessment,  
compliance, and  
insurance  
journey— every  
step of the way.**

### **Cybersecurity threatscape is constantly changing**

This makes the security space dynamic—there are no set-and-forget solutions. New gaps could open at any time in your cybersecurity strategy. Another critical element of maintaining your organization's security is regularly monitoring for changes or threats that could affect your network's security posture.

This includes keeping up with industry news and developments related to cyber threats as well as staying on top of patches and updates for existing software and hardware solutions used within the organization's network environment. It also means implementing appropriate logging practices so that any suspicious activity can be quickly identified and addressed before it has a chance to cause severe damage or disruption.

Attempting to conduct a comprehensive risk assessment and continuously keep up to date with threats is extremely difficult to do on your own.

### **Even if you have already done research**

There are still so many threats that you aren't even aware of that could harm your organization. That's why many organizations rely on large cybersecurity teams of employees who have specialized knowledge in a variety of cyber areas.

Unfortunately, not every organization can afford a complete IT security team of professionals who are currently in high demand. However, Trava Security changes the game. With our comprehensive assessment platform, you can rapidly get actionable intelligence about your current security posture. We make it easy to identify any gaps in your security and close them. We also provide a comprehensive suite of services that enable you to use the expertise of live professionals without having to invest in the expense of full-time employees.

---

**Still see this process as being overwhelming?** Trava can also help. Your cybersecurity needs are unique and require unique solutions. Cybersecurity doesn't have to be complicated. We'll prove it.

talk to trava