

# How to become more cybersecurity



Your company is at risk, regardless of its size or industry. SMBs are especially vulnerable because cybercriminals view them as easy targets with low or no defenses in place.

**In 2019, three in four SMBs in the U.S. had reported a digital attack in the preceding year**, according to Ponemon Institute. You just don't hear about them because attacks on smaller businesses don't make news like those involving global brands.

Successful cybersecurity protection is a three-pronged approach that takes into consideration your people, processes and technologies. Let's look at all three:



## People

Your workforce will always be your weakest link, but also can be your most potent weapon. Ongoing training with an emphasis on ways of staying safe within the network can dramatically reduce your risk.



## Processes

Defining and enforcing security practices are the basis for good cyber hygiene. But it also includes a strong incident response plan, which is well-rehearsed and documented to minimize damage and downtime.



## Technology

Cybersecurity tools are evolving alongside cybersecurity threats and becoming more predictive. Keeping current is critical to staying safe.

## An ounce of prevention is worth a pound of cure

At TPx, many of our cybersecurity clients are SMBs. Sadly, most don't turn to us for help until they've already been attacked. One of these victims-turned-clients lost \$200,000 to ransomware just weeks after leadership asserted that the company was "too small to be at risk."

Not only is financial loss a consideration for shoring up defenses, but your company's reputation is also at stake, even for smaller organizations that don't get attention from headlines. When you get hacked, you will be legally required to inform every affected customer that their data may have been stolen.

The risk of a breach is very real, and the cost is very high — significantly higher than threat prevention, detection and remediation solutions that are affordably available to SMBs today.

### Our Security Solutions

- Firewalls
- Endpoints
- Backups
- Managed Detection & Response
- Security Advisory Services
- Security Training



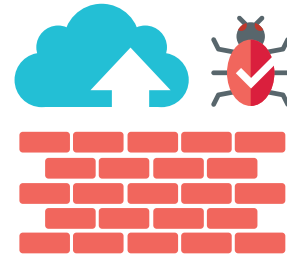
# 10 steps toward better cyber protection



Educate your staff by deploying quality cybersecurity awareness training.



Have a cybersecurity strategy that combines market-leading technology with seasoned expertise.



A solid endpoint security, firewall, and backup and recovery are a baseline.



Two-factor authentication and solid password controls are key for each employee.



Make sure staff has the appropriate level of access.



Test...  
test...  
test!



Make sure you have good visibility into an entire network.



Ensure your network is being monitored 24/7/365.



Remember...cybersecurity is where prevention beats mitigation.



Make sure your plan also covers cyber threat detection and response



## Want to learn more?

Download our free  
[Comprehensive  
Cybersecurity Guide for  
SMBs.](#)