6-STEP Cybersecurity Starter Guide for SMBs

6-STEP CYBERSECURITY STARTER GUIDE FOR SMBs

Computers and the internet bring many benefits to small businesses, but this technology is not without risks. Some risks, like physical theft and natural disasters, can be reduced or controlled through sensible behavior and commonsense precautions. Harder to handle are the cybercrime risks like those posed by criminals who steal information to sell on the black market.

63% of small/medium businesses experienced a data breach in 2019, according to a Ponemon Institute report. Yet, many proprietors believe they're not vulnerable to cyberattacks due to their small size and limited assets. Unfortunately, this is not the case.

This guide will help you defend your business against cybercrime threats.

Personal information is a common target of criminals. Even the smallest businesses are likely to handle some personal customer or vendor data worth stealing. Another popular target of cyber criminals is account information, including credit card data, bank account numbers, online banking passwords, email accounts, and user credentials for services such as eBay, PayPal and TurboTax.

All of these can be sold on the black market to other criminals who specialize in using the information in a wide range of fraud schemes and scams.

cyberattacks target small businesses

small and mid-sized businesses experienced eight or more hours of downtime due to cyber breach

Source: Agility SMB

CONSEQUENCES OF DATA THEFT

Because most small businesses have account information and personal data that criminals could abuse, you need to remember that your business may be held responsible for the consequences of data theft—for example, if information about your customers is stolen and used for fraud.

Some data is protected by laws and regulations, like **GDPR in the EU or CCPA in California.** Many states also require businesses to report security breaches that expose personal data to potential abuse, whether it's a lost laptop containing customer details, or a thumb drive with medical records.

All of this means that, even though your company may be small, you must take a **systematic approach to securing any data** that is entrusted to you. As you go about the task of protecting your company's digital assets, you should document your approach. This will help you **educate employees** about their security responsibilities.

Furthermore, it is not uncommon for larger companies to require vendors and contractors to provide proof that they have educated their employees about security, and that they have put appropriate security measures in place. If a security breach does occur, a documented security policy helps you prove that you were diligent in your efforts to protect information.

One third of the costs related to a data breach are incurred more than 1 year after the incident. Around **22%** of these costs are incurred in the second year.

source: ENISA

STEPS TO TAKE:

We've laid out a systematic approach to cybersecurity for you that goes from A to F.

- **A**ssess your assets, risks, resources
- **B**uild your policy
- **C**hoose your controls
- **D**eploy controls
- **E**ducate employees, execs, vendors
- **F**urther assess, audit, test

ASSESS YOUR ASSETS, RISKS, RESOURCES

ASSESS YOUR ASSETS, RISKS, RESOURCES

List all of the computer systems and services that you use. After all, if you don't know what you have, you can't protect it. Be sure to include mobile devices like smartphones and tablets that you and/or your employees may use to access company or customer information.

This is especially important **since 62% of 1,100 professionals** stated that they shortchanged mobile security for the sake of efficiency.[1]

And don't forget online services, such as SalesForce, online banking websites, and cloud services such as iCloud or Google Docs.

Now go through that list and consider the risks related to each item. Who or what is the threat? What are the risks related to remote working? Another good question to ask is: **What could possibly go wrong?** Some risks are more likely than others, but list them all and then rank them according to how much damage they could cause and the chances they might occur.

You might seek outside help with this process, which is why you need another list: **the resources you can tap for cybersecurity issues**. This could be someone on staff who is knowledgeable and security-savvy, or a partner or vendor. You can also oursource your cybersecurity to a managed service provider (MSP) which can provide the support you need.

62%

of professionals admitted they shortchange mobile security for the sake of efficiency

1) Source: Cyber Talk, March 2020

BUILD YOUR POLICY

BUILD YOUR POLICY

A sound security program begins with policy, and policy begins with **C-level buy-in**. If you're the boss, then you need to let everyone know that you take security seriously and that your firm is committed to protecting the privacy and security of all data that it handles.

Next, you need to spell out the policies that you want to enforce, for example, there shall be **no unauthorized access to company systems and data**, and employees will not be allowed to disable the security settings on their mobile devices.

You should define who has access to certain data within an organization, for what purposes, and what they are authorized to do with that data. It is also important to have policies about remote access, bring your own device (BYOD) or authorized software.


CHOOSE YOUR
CONTROLS

CHOOSE YOUR CONTROLS

You use controls to enforce policies. For example, to **enforce the policy of no unauthorized access** to company systems and data, you may choose to control all access to company systems with a unique username, password and some form of **two-factor authentication**.

To control **what programs are allowed** to run on company computers, you may decide not to give employees **administrative rights**. To prevent breaches caused by lost or stolen mobile devices, you could require employees to report such incidents the same day—and specify that such devices will be remotely locked and erased immediately.

At a minimum you will want to use these security technologies:

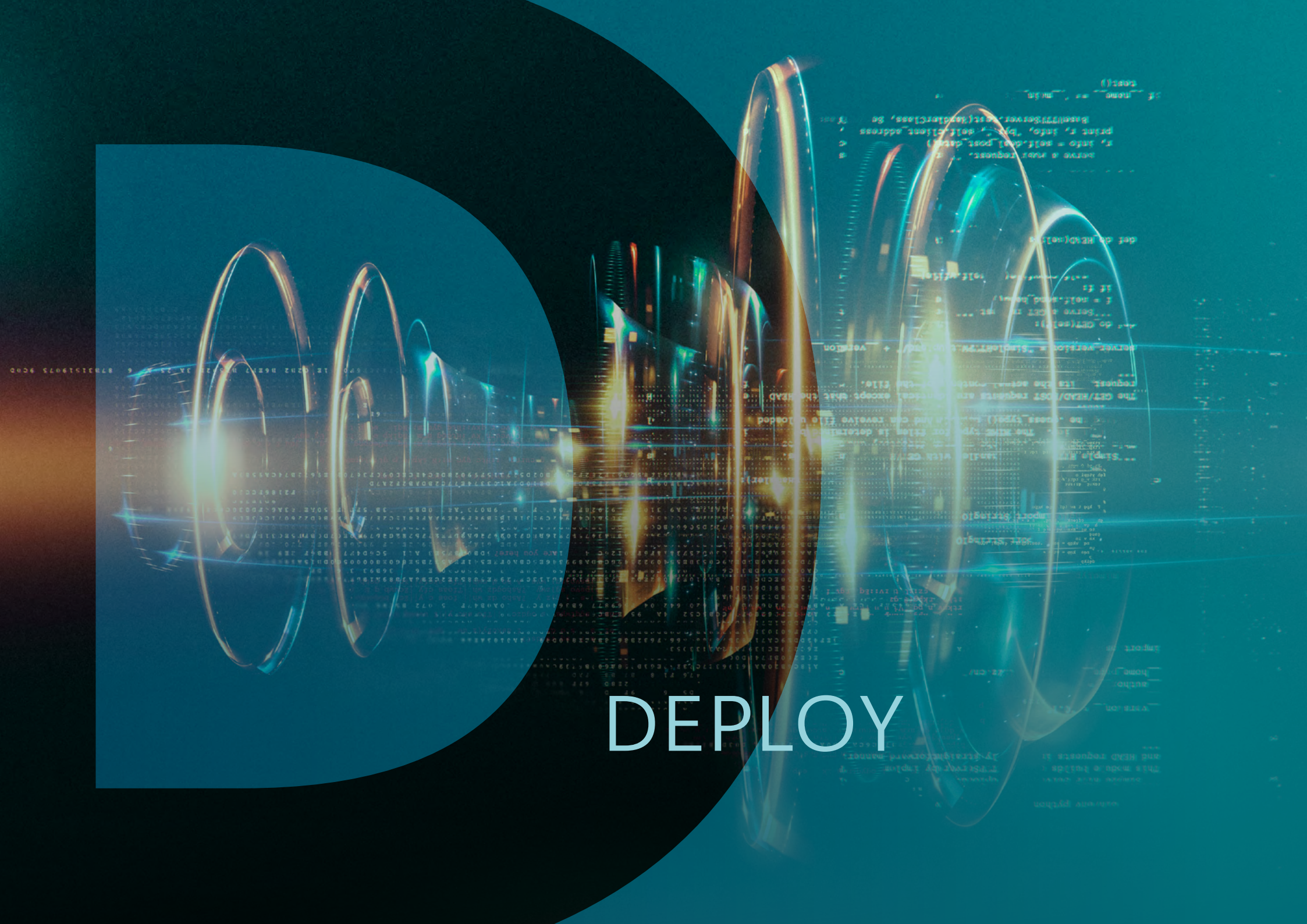
- **Endpoint protection solution** that will prevent malicious code from being downloaded onto your devices.
- **Encryption software** that will render data on stolen devices inaccessible, which is also suggested by the EU GDPR
- **A two-factor authentication** system, so that something more than just a username and password are required to gain access to your systems and data.
- **A VPN solution** that will add another layer of protection to remote working employees

Future proof your company IT security

Today's cybersecurity landscape is continually evolving, using sophisticated obfuscation techniques. The ultimate goal for malware actors is to remain unnoticed on the endpoint, evading antimalware detection by creating never-before-seen threats, or zero-days.

A cloud-based security sandbox provides a defensive layer outside a company's network to prevent ransomware from ever executing in a production environment. The suspicious file is blocked from execution on the endpoint.

eset®


DEPLOY

DEPLOY

When you deploy controls, make sure they work. For example, you should have a policy that prohibits unauthorized software on company systems; one of your controls will be **anti-malware software** that scans for malicious code.

Not only do you need to install this and test that it doesn't interfere with normal business operations, you also need to document the procedures you want employees to follow when malicious code is detected.

When choosing the right endpoint protection solution there are also a few key considerations to look for. For example, you want **the highest detection rates possible**, while the incidence of false positives (alerts on the files or links that aren´t actually malicious) should be as close to zero as possible. It also **shouldn´t have a noticeable impact on system performance** and should be easy to manage and maintain.

Endpoint security management console

When deploying endpoint protection, you want to have an overview of all your endpoints on a single-pane-of-glass. A cloud console such as ESET PROTECT offers this functionality.

It ensures real-time visibility for on-premises and off-premises endpoints as well as full reporting and security management for all OSes.

It controls endpoint prevention, detection and response across all platforms—covering desktops, servers, virtual machines and even managed mobile devices.

LEARN MORE


EDUCATE

EDUCATE

Your employees need to know more than just the company security policies and procedures. They also need to understand why these are necessary. This means **investing in security awareness and education**, which is often the single most effective security measure you can implement.

By working with your staff, you can raise awareness of issues such as phishing email. A study showed that 43% of employees are not even sure what a phishing attack is[2].

Therefore, prepare regular training for your employees, for example, a phishing quiz, to teach them which techniques malicious actors are using. Make cybersecurity awareness part of the onboarding process and provide security tips on an intranet page.

Be sure to educate everyone who uses your systems, including executives, vendors, and partners. And **remember that violations of security policies must have consequences**. Failure to enforce policies undermines the whole security effort.

ESET's **free online cybersecurity awareness training** is an easy and effective way to educate your workforce. It takes under 60 minutes to complete and covers topics from phishing and password policies to remote workplace security.

GET STARTED NOW

69%

of organizations were breached due to an insider threat, despite preventive measures[3]

2) Source: ZD Net, Oct 2020
3) Source: Sapio Research Study, UK

FURTHER ASSESS, AUDIT, TEST

FURTHER ASSESS, AUDIT, TEST

Cybersecurity for any business, large or small, is an ongoing process, not a one-time project. You should plan on **re-assessing your security on a periodic basis**, at least once a year.

You may need to update your security policies and controls more than once a year depending on changes to the business, such as **new vendor relationships, new projects, new hires, or employees departing** (making sure that all system access is revoked when anyone leaves the company). Consider hiring an outside consultant to **perform a penetration test and security audit** to find out where your weak points are and address them.

The current wave of cybercrime is not going to end any time soon, so you need to make an ongoing good faith effort to protect the data and systems that are the lifeblood of today's small business.

To stay up to date on emerging threats, review security news on a regular basis by subscribing to websites like:

WeLiveSecurity.com

DataSecurityGuide.eset.com

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.