TeamsID

Lean Security Checklist

INTRODUCTION

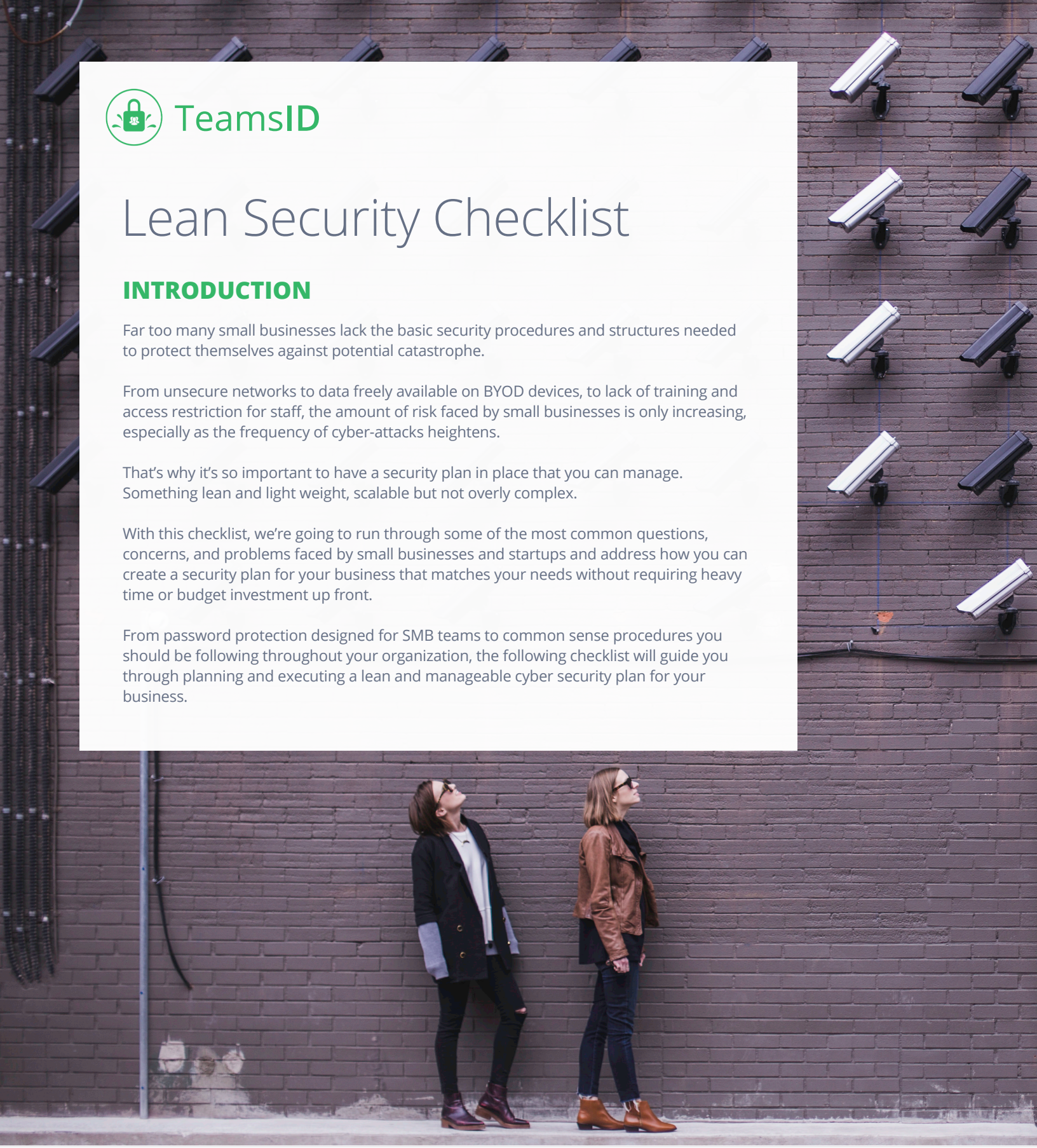
Far too many small businesses lack the basic security procedures and structures needed to protect themselves against potential catastrophe.

From unsecure networks to data freely available on BYOD devices, to lack of training and access restriction for staff, the amount of risk faced by small businesses is only increasing, especially as the frequency of cyber-attacks heightens.

That's why it's so important to have a security plan in place that you can manage. Something lean and light weight, scalable but not overly complex.

With this checklist, we're going to run through some of the most common questions, concerns, and problems faced by small businesses and startups and address how you can create a security plan for your business that matches your needs without requiring heavy time or budget investment up front.

From password protection designed for SMB teams to common sense procedures you should be following throughout your organization, the following checklist will guide you through planning and executing a lean and manageable cyber security plan for your business.



SECURITY MUSTS CHECKLIST FOR STARTUPS & SMBS

Next Page

TeamsID

SECURITY MUSTS FOR STARTUPS & SMBS

Before looking at potential gaps in security, there are some fundamentals that every small business should have in place. Basic security steps that will protect against every day intrusions and employee mistakes.

These are the things that should be in place by default and maintained as your team grows. Much of these security basics can be automated and scaled with software and MSP support, but for a small and growing business, an eye for attention and a calendar app will often get the job done. The key is to have someone whose job it is to oversee updates and audits of each part of this process.

FIREWALL

On premise hardware should be protected by firewall managed by a system administrator or MSP. A good firewall will recognize potential threats, stop risky activity by employees, and restrict unnecessary or unapproved file transfers and login attempts. While most systems have default firewalls these days, it's important to customize and enhance these systems to match your business needs.

ANTIVIRUS

Antivirus is not built into computer systems, meaning the vast majority of small businesses remain unsecure. A good antivirus program should be installed on all workplace computers, updated at regular intervals (preferably with automatic updates at the end of each business day), and tested frequently. Modern antivirus does more than protect against devastating viruses. They monitor for and remove adware and malware that can open the door to outside intrusion and ransomware attacks. This includes scanning downloaded files, email attachments and installable .exes.

PATCHES & UPDATES

A good patch policy is a must. The average business computer has more than 30 pieces of regularly updated software on it. Any one of these, if it connects to the Internet, can be a potential security hole if not updated properly. Even with many business applications moving to the cloud, desktop software remains a huge potential risk for small businesses that use often outdated operating systems, office software, and email clients. Make sure your OS is fully supported by the software's manufacturer as well – old versions of Windows are one of the reasons the Wannacry attack spread so wide this spring.

INTRUSION PREVENTION

A good firewall, up to date virus protection, and patch update policy will go a long way towards intrusion prevention in your systems. If you store high value information or confidential data, you may want to go an extra step for network monitoring software that will help to identify potential intrusions and take action in the case of one being detected.

WEB FILTERS & ACCESS CONTROL

If your employees are using business computers, it's important to monitor and control their access to potentially harmful sites that could contain spyware, malware, or viruses in the form of cookies, downloadable files, or corrupted images. Web filters that block untrusted sites, minimize non-work activity, and trigger alerts when something suspect is downloaded or accessed are highly recommended.

VPN

A virtual private network is yet another way to protect against outside access, virtualizing the IP address for a place of business and making it harder to access through automated routines – the methods used in most hacking attacks.

DATA LOSS PREVENTION

Hacking and malicious attacks may get all of the headlines, but the biggest risk for small businesses is data loss. Pure destruction in the form of a virus, corruption of a machine, or simple damage are all problems that can be avoided by having an off-site backup of all data in the cloud. For sensitive data, on-site cloud backup or hard drive backup is more affordable than ever before.

TRAINING

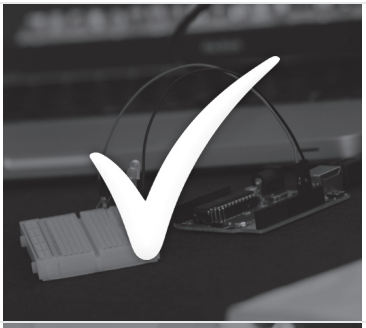
Finally, there is training. For each new system installed or updated, your team needs to know why it was installed, what your expectations of them are, and the consequences of not following the updated procedures you've now put in place.

TeamsID

IDENTIFYING GAPS IN YOUR SECURITY

Once you've established the fundamentals in your security plan, it's time to evaluate your organization for potential holes. These are hardware and software gaps that can lead to potential risk, and human error that often gets overlooked.

Gaps in security are not one-time fixes, however. While some things, like IoT security can be addressed in one go, most of these require ongoing training and oversight to ensure there are no issues. Policies that address these issues are recommended to reduce the potential for future attacks due to human error.



UP-TO-DATE MISSION CRITICAL SOFTWARE/HARDWARE

Even if you have a patch policy that ensures every system is checked once a month for recent updates, there may be times when a vital security update comes through that needs to be installed sooner. Employees who don't turn off or restart their machines or software that doesn't reliably auto-update can get missed in these instances and someone needs to be paying enough attention to know that an update is needed.

EMPLOYEE TRAINING PROCESSES/MANUAL

Your current employee training is likely lacking in the basic security procedures needed to protect your business from breach and data loss. It's recommended that you review and possibly rewrite your policies for both new employees during onboarding and existing employees who will need to be up to date on your new policies. Frequent retraining is recommended as procedures are updated or new challenges arise.

ADMIN ACCESS & DEVICE ACCESS

Few people in your organization need full admin access to any of your device or software resources. Unchecked admin access combined with the risk of human error greatly increases the number of opportunities for a breach to occur. Restrict access where it isn't needed and manage it carefully for all new machines and devices installed in your office.

MOST RECENT BACKUP DATE/TIME

When was the last time a full backup was completed for your mission critical systems? If you haven't yet installed an automated backup system, make sure you have a regular backup in place so that you never lose a substantial amount of data that could slow or hurt your business performance.

IOT PASSWORD SECURITY

IoT devices are among the biggest security holes in your office right now. Printers and scanners in the workplace, and just about anything connected to the Internet in your home – from your refrigerator to a stray camera – can be a potential access point to your network and in turn your data. Most IoT devices come with blank passwords by default. Update these upon installation to avoid easy access from outside sources.

MOBILE & BYOD POLICIES

The modern employee is more likely to use their own devices than a business-provided laptop or phone. To avoid this becoming a major liability, have a clearly outlined BYOD and mobile policy in place. If you have one already, review it and check to ensure it is being adhered to. Employees with sensitive business information on their devices that are not protected nearly as well as business machines are a major risk for many businesses.

TeamsID

SCALING YOUR SECURITY WITH GROWTH

Addressing the issues in this checklist is only part one of ensuring a safe and secure business environment. Long term risk assessment and management is required to reduce the opportunity for cyber-attack.

With growth, your business will integrate new technologies, a much larger workforce, and new policies that all pose challenges in keeping up with your cyber concerns. Some of these ongoing issues include:

BYOD

Bring your own device policies are vital at all stages of business. It's incredibly difficult to manage who uses a personal phone or computer for work purposes, and more so to demand that they don't outside of highly sensitive industries. To avoid compliance being a major issue, initiate a proactive and scalable policy that allows you some latitude over how secure these devices are.

REMOTE EMPLOYEES

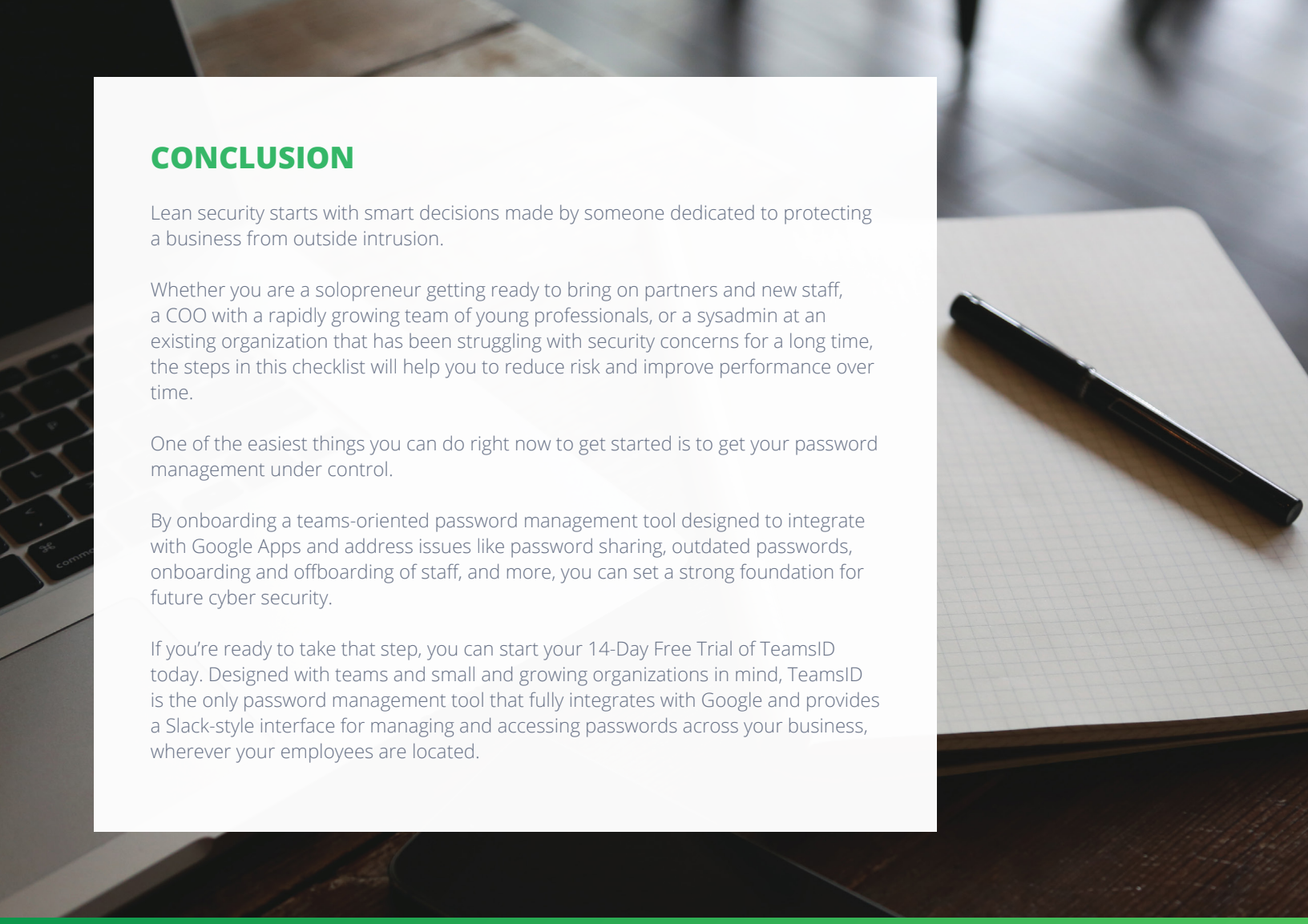
Another common trend in modern business is remote workforces. Remote employees or contractors may have access to the same sensitive data that you are so carefully protecting in the office. Cloud password management, data access control, and policy reviews for data security are all vitally important in such cases.

RELIABILITY & LONGEVITY OF SAAS

Cloud-based SaaS products are a great way to offload a lot of the security concerns over how your data is managed and backed up. At the same time, you need to know that the companies you select are reliable with a long track record of security prioritization, no major hacks, or data breaches. Longevity is another issue. If the company has a history of short lived products or M&A is rampant in an industry, it can be difficult to trust that your tools of choice will still be there in few months or years as you grow. Have backup plans in place.

INTEGRATION WITH OTHER SYSTEMS

How do your chosen tools and systems integrate with other systems? New tools may offer a bevy of features, but if they are not fully integrated with the email systems you use or your file storage of choice, they may not be as flexible (or secure) as you would like.



CONCLUSION

Lean security starts with smart decisions made by someone dedicated to protecting a business from outside intrusion.

Whether you are a solopreneur getting ready to bring on partners and new staff, a COO with a rapidly growing team of young professionals, or a sysadmin at an existing organization that has been struggling with security concerns for a long time, the steps in this checklist will help you to reduce risk and improve performance over time.

One of the easiest things you can do right now to get started is to get your password management under control.

By onboarding a teams-oriented password management tool designed to integrate with Google Apps and address issues like password sharing, outdated passwords, onboarding and offboarding of staff, and more, you can set a strong foundation for future cyber security.

If you're ready to take that step, you can start your 14-Day Free Trial of TeamsID today. Designed with teams and small and growing organizations in mind, TeamsID is the only password management tool that fully integrates with Google and provides a Slack-style interface for managing and accessing passwords across your business, wherever your employees are located.