Checklist

30 Things to Check in Your Business to Improve Your Cybersecurity

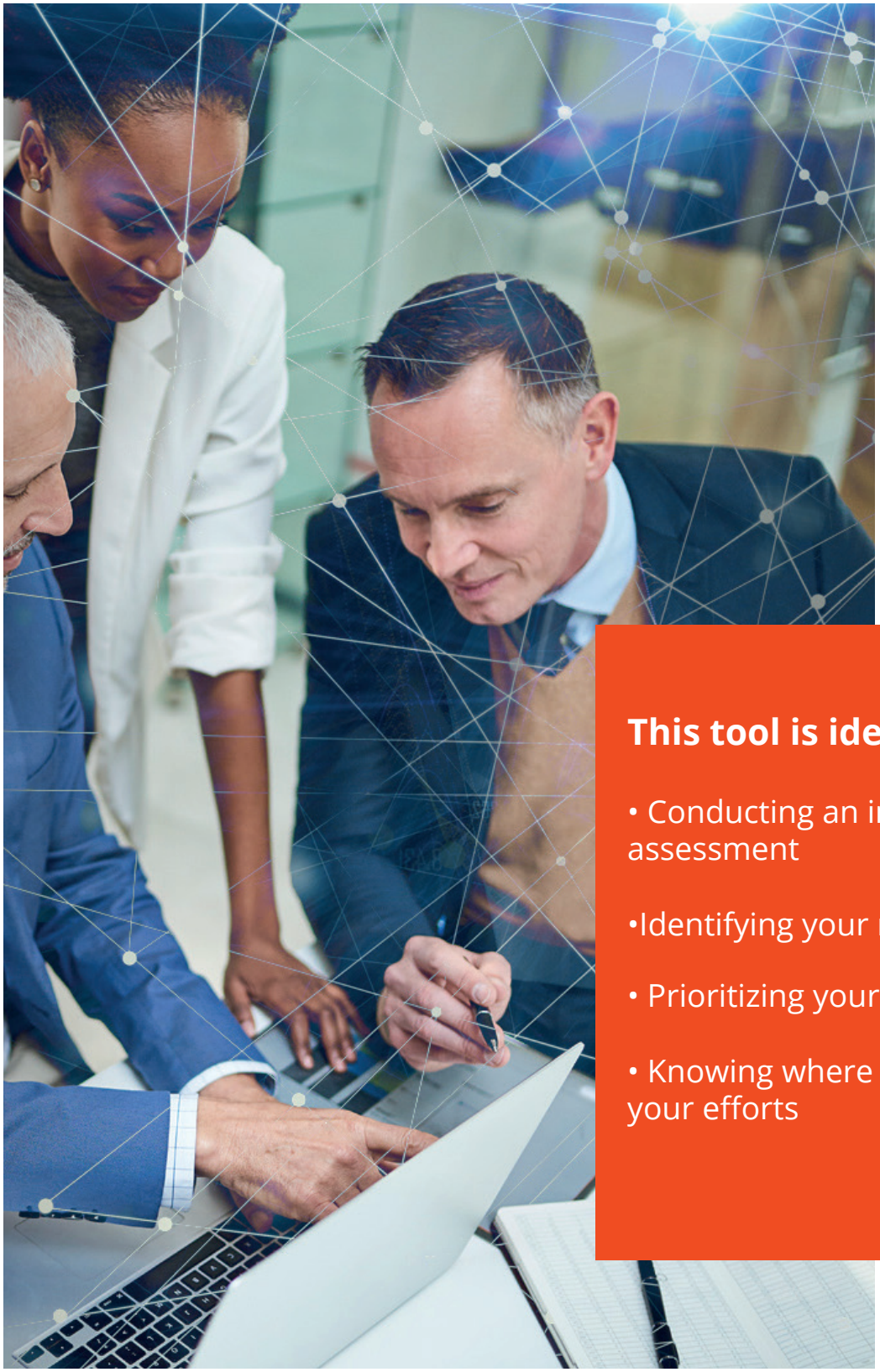
ABAKUS
IT-SOLUTIONS

Did you know that the majority of cyberattacks targeting SMBs don't come from sophisticated techniques?

In recent years, we've seen a sharp increase in cyberattacks. Outdated software, weak passwords, misconfigured Wi-Fi, incomplete backups, outdated firewalls...
And it's SMBs, being less protected, that have the most to lose.

The problem?
Most business leaders think they're protected, until the day an incident occurs. And in 70% of cases, post-incident analysis reveals that a few simple measures could have prevented the disaster.

What if you took these measures now?
This checklist compiles 30 essential points, drawn from our field experience, which allow you to assess your company's security level.



This tool is ideal for:

- Conducting an initial assessment
- Identifying your risk areas
- Prioritizing your actions
- Knowing where to focus your efforts

30 things to check in your business

NETWORK & INFRASTRUCTURE

- ◯ Is a firewall present and properly configured on the network?
- ◯ Are the firewall's security licenses (IPS, antivirus, web filtering) active and up to date?
- ◯ Do remote connections use a secure VPN such as IPsec?
- ◯ Is multi-factor authentication (MFA) enabled for VPN access?
- ◯ Are security logs retained for a sufficient period (at least 4 to 6 months)?
- ◯ Is the network segmented to isolate sensitive or vulnerable equipment?
- ◯ Is a «Guest» Wi-Fi network separate from the internal network in place?
- ◯ Does the internal Wi-Fi use secure encryption such as WPA2/WPA3 Enterprise?
- ◯ Is Wi-Fi access linked to user accounts via a RADIUS server?
- ◯ Are servers physically protected (secure cabinet, restricted access)?

SYSTEMS, WORKSTATIONS & SERVERS

- ◯ Are the operating systems of servers and workstations up to date and still supported by the vendor?
- ◯ Is regular maintenance (security patches, CVE fixes) ensured?
- ◯ Is professional antivirus software installed on all workstations and servers?
- ◯ Are antivirus events and alerts monitored and analyzed?
- ◯ Is an EDR (Endpoint Detection & Response) solution in place?
- ◯ Are workstation hard drives (especially laptops) encrypted?
- ◯ Are workstation applications updated automatically?
- ◯ Do users have only the strictly necessary rights (least privilege)?
- ◯ Are local administrator rights removed or managed via a secure solution (e.g., LAPS)?
- ◯ Is multi-factor authentication (MFA) enabled for access to critical systems?

DATA, BACKUPS & CONTINUITY

- ◯ Is a backup strategy following the 3-2-1 rule in place?
- ◯ Are backups encrypted and protected against unauthorized access?
- ◯ Are regular backup restoration tests performed?
- ◯ Is centralized data (servers, SharePoint, shared files) backed up?
- ◯ Is non-centralized data (user workstations) also protected?
- ◯ Is M365 data (Exchange, Teams, SharePoint) backed up by a dedicated solution?
- ◯ Does a disaster recovery plan (DRP) exist and is it documented?
- ◯ Is a cloud disaster recovery solution (DRaaS) planned?

ORGANIZATION, USERS & GOVERNANCE

- ◯ Does a formalized IT security policy exist and is it communicated to users?
- ◯ Are users trained and regularly made aware of cyber risks (phishing, best practices)?

What Abakus can do for you in cybersecurity

ABAKUS is your complete IT partner.

We support businesses in their various IT needs: talent recruitment, infrastructure management, tool implementation...

In cybersecurity, we help you transform the checks in this checklist into a real action plan tailored to your business.
Our experts conduct a comprehensive analysis of your environment, identify your vulnerabilities, strengthen your infrastructure, and implement essential best practices to reduce your risks.

Our objective?
Make your business more resilient, more secure, and better prepared against current threats.

4 DIVISIONS TO MEET YOUR IT NEEDS

At ABAKUS, we believe that all businesses deserve IT comfort.
We help you achieve it through a diversity of services.

IT Consulting

Expert support for your IT projects, including governance, talent selection, and development and cybersecurity consulting.

Infrastructure Management

Complete supervision of your infrastructure, from cloud to support, including network, backup, and maintenance.

Odoo Implementation

Design and deployment of custom Odoo solutions, including Python/API development and business optimization.

Cybersecurity

Governance, compliance, and protection of your systems through audits, risk management, and operational security.