



Here are some of the **biggest cybersecurity problems** facing small and medium-sized enterprises (SMEs) right now (2025) — plus notes on *why* they're issues and some pointers for mitigation. Since you're working with SMEs (albeit in accessories / e-commerce) this should help frame your thinking.

1. Limited resources + lack of specialised expertise

- Many SMEs simply don't have the budget or staff to build an in-house security team, monitor 24/7, or stay on top of evolving threats. SCIRP +2
- They may also lack awareness or cybersecurity literacy: what threats exist, how to detect, how to respond. arXiv
- Because of that, SMEs often are easier targets for attackers (less "hardening"). NCX Group

Why it matters: If your business is digitally active (webshop, payment integration, cloud infrastructure) these limitations create gaps attackers can exploit.

Pointers: Prioritise core controls (patching, backups, strong passwords, multi-factor authentication), consider outsourcing to a managed service for security monitoring, allocate budget for regular training / awareness for your staff.

2. Phishing, social engineering & human error

- Phishing remains one of the top entry vectors for attackers targeting SMEs. Cyber Tech Guar... +2
 - Human error (clicking malicious link, weak password, mis-configured cloud share) remains a big vulnerability. IT Pro +1
- Why it matters:** Regardless of how good your technology is, if people are not trained or aware, attackers will exploit that "weak link".

Pointers: Run basic training with your team (even small team), phishing-simulations (if possible), enforce MFA for all key systems, adopt principle of least privilege (so a single error doesn't lead to full compromise).

3. Ransomware & extortion-type attacks

THE PROBLEM
WITH CYBERSECURITY
podla ChatGPT



5. Supply-chain, third-party & vendor risks

- SMEs may not only be targets themselves, they also may be weaker links in the supply chain of larger organisations. Attacks through third-party vendors or software dependencies are rising. securityexception... +1

Why it matters: Even if your systems are relatively secure, if you integrate with or depend on other vendors/suppliers who are not, you may still get compromised via them.

Pointers: Evaluate your vendors: their security practices, what access they have to your systems/data. Limit vendor permissions to “just enough”. Include security clauses in vendor contracts. Monitor vendor access.

6. Lack of incident-response preparedness & resilience

- Many SMEs do not have formal incident-response plans, lack testing of backup/restoration, or lack continuity planning. IT Pro +1

Why it matters: If you *are* breached, your ability to respond, recover, restore operations will determine how much damage you suffer.

Pointers: Create a basic incident response plan (who does what when you detect a breach), perform tabletop exercises even informally, ensure you know how you’ll communicate (internally + externally), know which backups you’ll restore and how.

7. Evolving / sophisticated threats (AI-powered, targeted)

- Attackers are adopting more advanced tactics: AI-driven phishing, highly-targeted attacks, etc.

WardenShield +1

Why it matters: What used to be low-hanging fruit is evolving. If you assume “we’re too small to be noticed”, that’s a dangerous mindset.

Pointers: Stay up to date with threat intelligence at least at a high level, ensure you have layers of defence (not just one security control), consider adopting “detect and respond” mindset not just “prevent”.

8. Regulatory/compliance burdens & business risk awareness

- In many jurisdictions (especially EU) SMEs are increasingly subject to regulations (data protection, breach reporting, etc). Also cybersecurity is a **business risk** (not just an IT issue) — leadership awareness is still often lacking. The Times +1

Why it matters: If you treat cybersecurity only as “IT’s job”, you may miss bigger business-impact issues: e.g., reputational damage, customer trust, supply-chain compliance, liability.

Pointers: Elevate cybersecurity to board/leadership level (even if small business). — ensure someone is

THE PROBLEM WITH CYBERSECURITY podla ChatGPT



COMPLIANCE CYBERSECURITY

**Ako môže softvérová
platforma s AI vylepšiť
výkon manažérov
kybernetickej
bezpečnosti**



Problém:
vyriešiť súlad s legislatívou a popri tom aj
reálne zlepšiť bezpečnosť.
Za rozumné náklady.

Legislatíva 1

Zákon o KB / NIS2:

- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

GDPR (roadmapa)

DORA (roadmapa)



ITACON - test

Pavol Rybár

← Úprava dopadov

Ekonomický systém Pohoda

Informačný systém

Hlavné aktívum

56

INHERENTNÉ RIZIKO

45

FINÁLNE REZIDUÁLNE RIZIKO

Vyhľadať

Vyhľadať

Rozšírený filter

DOPAD	KATEGÓRIA DOPADU	ÚROVEŇ DOPADU
Dopad na klientov	Klienti	✓
Dopad v prípade nedostupnosti	Dostupnosť	✓
Dopad v prípade straty všetkých údajov	Dostupnosť	✓
Dopad v prípade zverejnenia mimo organizáciu	Dôvernosť	✓
Prevádzkový dopad externý		

Riziká

Aktíva

Implementované opatrenia

Filter:

Aktíva

Riziká

Opatrenia

Analytické prehľady

Report riadenia rizík

RIZIKO	KATEGÓRIA HROZBY	MAX. INHERENTNÉ RIZIKO	MAX. REZIDUÁLNE RIZIKO
Fyzická krádež alebo fyzické poškodenie zariadení alebo médií	Fyzické hrozby	56	56
Chyba alebo zlyhanie obsluhy, údržby alebo zamestnanca vykonávajúceho podporné služby	Ľudské konanie	56	45
Infiltrácia komunikácie	Kompromitácia údajov alebo služieb	70	14
Neautorizovaná manipulácia so SW alebo hackerský útok	Kompromitácia údajov alebo služieb	70	14

Legislatíva 2

Zákon o KB / NIS2:

- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

GDPR (roadmapa)

DORA (roadmapa)



Úprava rizikového profilu

Websupport s.r.o.

Zrušiť

Uložiť

Úroveň dôvernosti dát zdieľaných s treťou stranou.

☐ žiadna ☐ interné ☐ chránené ☐ prísne chránené

Úroveň dostupnosti dát zdieľaných s treťou stranou.

☐ žiadna ☐ nízka ☐ stredná ☐ vysoká

Úroveň integrity dát zdieľaných s treťou stranou.

☐ žiadna ☐ nízka ☐ stredná ☐ vysoká

Úroveň citlivosti dát zdieľaných s treťou stranou.

☐ žiadne citlivé údaje ☐ telekomunikačné/bankové tajomstvo ☐ obchodné tajomstvo/osobné údaje ☐ špeciálna kategória osobných údajov/zdravotné záznamy

Hodnota kontraktu s treťou stranou.

☐ žiadna ☐ zanedbateľná ☐ významná ☐ značného rozsahu

Zmenové požiadavky

Vytvoriť zmenovú požiadavku

Vplyv tretej strany

☐ žiaden ☐ ...

Vyhľadať

Vyhľadať

Rozšírený filter

x

Rozsah komunikácie

☐ žiaden ☐ ...

Vplyv spolupráce

☐ žiaden ☐ ...

Potenciál uloženia

☐ žiaden ☐ ...

ID	ZMENOVÁ POŽIADAVKA	STAV	DÁTUM A ČAS ŽIADOSTI	DÁTUM A ČAS PRIJATIA/ZAMIETNUTIA	ŽIADATEĽ	
2025/1	Change FW configuration - new Backup service for POHODA	Návrh	19.5.2025 09:25:00	-		
2025/2	Zmena úrovne AD	Schválené	11.11.2025 16:59:00	18.11.2025 16:59:00	Ivana Pukajová	

Legislatíva 3

Zákon o KB / NIS2:

- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

GDPR (roadmapa)

DORA (roadmapa)



Stratégia obnovy

Vyhľadať

Vyhľadať

Rozšírený filter

☐ NÁZOV AKTÍVA ^	TYP AKTÍVA ↕	HLAVNÉ AKTÍVUM ↕	RTO ↕	RPO ↕
☐ Economic software - Omega	Aplikačný softvér	✓	do 3 dní	24 hodín
FW-PA-460	Sieťová infraštruktúra		do 3 dní	24 hodín
☐ Systém zákazníckej podpory (AI)	Informačný systém	✓	-	-
☐ Tazilla app	Aplikačný softvér	✓	do 24 hodín	8 hodín

← BCP - Omega

Nový test plánu

Plán

BCP

Prehľad

Aktíva

Testy plánu

Súbory

NÁZOV ^	POPIS ↕	TYP TESTU ↕	DÁTUM ↕	VÝSLEDOK ↕	
BCP Test Omega	Test prebehol úspešne	Simulácia	12.5.2025	Úspešné	
BCP test Omega pravidelný	-	Simulácia	31.12.2025	Plánované	

Legislatíva 4

Zákon o KB / NIS2:

- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

GDPR (roadmapa)

DORA (roadmapa)



Tazilla

Dashboard

Organizácia

Profil organizácie

Zamestnanci

Používateľské účty

Základné služby

Dokumentácia

Analýza rizík

Riadenie kontinuity

Registre

Riadenie súladu

Vzdelávanie

Dokumentácia

Generovať

Nahrať novú sadu dokumentov

Vyhľadať

Vyhľadať

Rozšírený filter

SADA DOKUMENTOV	KATEGÓRIA	DÁTUM	
Cyber security audit report 2024	Externý audit	26.12.2024	
End user computing	Smernica	10.3.2025	
End user security policy	Smernica	1.5.2025	
Identity and access management	Smernica	9.9.2025	
Information Security Risk Management	Smernica	11.9.2025	
Physical security	Smernica	1.12.2024	
Physical security	Smernica	18.6.2025	
Security incident management	Smernica	5.5.2025	
Third Party Risk Management	Smernica	1.7.2025	

Vzory smerníc

Názov

Bezpečnostná politika

Názov

Riadenie bezpečnostných incidentov

Názov

Stratégia informačnej a kybernetickej bezpečnosti

Ochrana údajov a súkromia

Školenie

Ukončené

Prehľad

Názov:

Téma:

Jazyk:

Stav:

Dátum od:

Dátum do:

Požadovaná úspešnosť:

Počet otázok:

Ochrana údajov a súkromia



← Data Protection & Privacy

Školenie

Ukončené

← Späť do Prebieha

Pridať účastníkov

Prehľad Účastníci

Vyhľadať

Vyhľadať

Rozšírený filter



MENO A PRIEZVISKO	E-MAIL	ORGANIZAČNÁ JEDNOTKA	STAV ŠKOLENIA	SKÓRE TESTU	POZVÁNKA ODOSLANÁ	ZAČIATOK SPRACOVANIA TESTU
Jozef Stanko	jozef.stanko@itacon.sk	-	Prebieha	-	9.10.2025 19:00	9.10.2025 19:03:53
Martin Ďurina	martin.durina@itacon.sk	-	Ukončené	100	-	10.10.2025 11:02:06

Reálna bezpečnosť: vzdelávanie 1

Plán vzdelávania

Školenia zamestnancov

Oboznamovanie sa

← Updating the KYB Strategy

Potvrdiť oboznámenie sa

Tazilla EN s.r.o. (EC)

Dostupné do: 30.5.2026

Please review the attached policy, with particular attention to the amendments in Section 3, and confirm your acknowledgment. Thank you.

Dokumenty:

 Cybersecurity Strategy.pdf

Updating the KYB Strategy

✓ Ukončiť oboznamovanie sa

Pridať účastníkov

Oboznamovanie sa

Prebieha

hľad

Účastníci

Súbory

hľadať

 Vyhľadať

 Rozšírený filter

MENO A PRIEZVISKO	E-MAIL	ORGANIZAČNÁ JEDNOTKA	STAV	DÁTUM A ČAS POTVRDENIA	POZVÁNKA ODOSLANÁ	
External Subject	external@yopmail.com	-	Nepotvrdené	-	28.5.2025 11:52	
Jozef Stanko	jozef.stanko@itacon.sk	Security dept.	Potvrdené	-	27.5.2025 09:27	
Lucia Fábryová	lucia.fabryova@itacon.sk	Security dept.	Nepotvrdené	-	27.5.2025 08:56	

Reálna
bezpečnosť:
vzdelávanie 2

Plán vzdelávania
Školenia zamestnancov
Oboznamovanie sa

Reálna bezpečnosť: zraniteľnosti 1

Threat intel
Skenovanie zraniteľností
Analýza kódu



Threat intelligence

Dátum skenovania: 17.11.2025 18:00:18

- Dashboard
- Prehľad
- Názvy hostov
- Rizikové ukazovatele 3
- Zraniteľnosti 406
- Webové certifikáty
- Porty 7
- Produkty
- Web technológie

Celkové riziko

Zobrazíť všetky

89 %

Zraniteľnosti

Zobrazíť všetky

91
Nízka

124
Stredná

154
Vysoká

37
Kritická

Najvyššia úroveň zraniteľnosti: ↑ 100 %

Najnižšia úroveň zraniteľnosti: ↓ 8 %

Najviac zraniteľné IP adresy: 37.9.175.179

Certifikáty

Zobrazíť všetky

Rizikové ukazovatele

Zobrazíť všetky

Threat intelligence

Dátum skenovania: 17.11.2025 18:00:18

- Dashboard
- Prehľad
- Názvy hostov
- Rizikové ukazovatele 3
- Zraniteľnosti 406
- Webové certifikáty
- Porty 7
- Produkty
- Web technológie

KÓD ^	POPIS ↕	ÚROVEŇ OHROZENIA ↕	POČET HOSTOV ↕	IP ADRESY
database	Zverejnené alebo verejne prístupné databázové služby. Môžu byť cieľom útokov SQL injection alebo krádeže dát.	Vysoká	1	37.9.175.179
eol-product	Zariadenia s neaktualizovaným softvérom alebo hardvérom, ktorý už nie je podporovaný výrobcom. Predstavuje bezpečnostné riziko.	Kritická	1	37.9.175.179
starttls	Zariadenia podporujúce príkaz STARTTLS na prechod z nezabezpečeného pripojenia na zabezpečené TLS pripojenie. Nesprávna konfigurácia môže vystaviť spojenie útokom typu downgrade.	Stredná	1	37.9.175.179

Reálna bezpečnosť: zraniteľnosti 2

Threat intel

Skenovanie zraniteľností

Analýza kódu



?

Tazilla EN s.r.o. (EC) ▾

Pavol Rybár ▾

 Dashboard

 Organizácia ▾

 Analýza rizík ▾

 Riadenie kontinuity ▾

 Registre ▾

 Riadenie súladu ▾

 Vzdelávanie ▾

 Ďalšie služby ▴

Threat intelligence

Skenovanie zraniteľností

Analýza kódu

Honeypot

← Tazilla safe scan

Sken zraniteľností

Safe scan

Vytvorený

Prehľad

Výsledky

ID:

2025/1

Názov:

Tazilla safe scan

Stav:

Vytvorený

Typ skenu:

Safe scan - Neinvazívne skenovanie zraniteľnosti

Dátum a čas začiatku:

26.5.2025 13:46:00

Dátum a čas nasledujúceho skenovania:

-

Zoznam hostov:

www.tazilla.com

Porty:

Všetky IANA priradené TCP

Interval opakovania:

Neopakuje sa

▶ Spustiť

⋮



Honeypot

[Attack overview](#)

[Attack source](#)

[Vulnerabilities overview](#)

[Honeypot interactions](#)

Date/time from

Date/time to

mm / dd / yyyy , -- : --

mm / dd / yyyy , -- : --

Filter

Clear filter

NAME ^

SEVERITY ↕

COUNT ↕

Attempted Administrator Privilege Gain

Critical

40

Attempted Denial of Service

High

3

Showing 1-2 of 2

«

<

Page 1 of 1

>

Reálna bezpečnosť: prevencia a detekcia

Honeypot

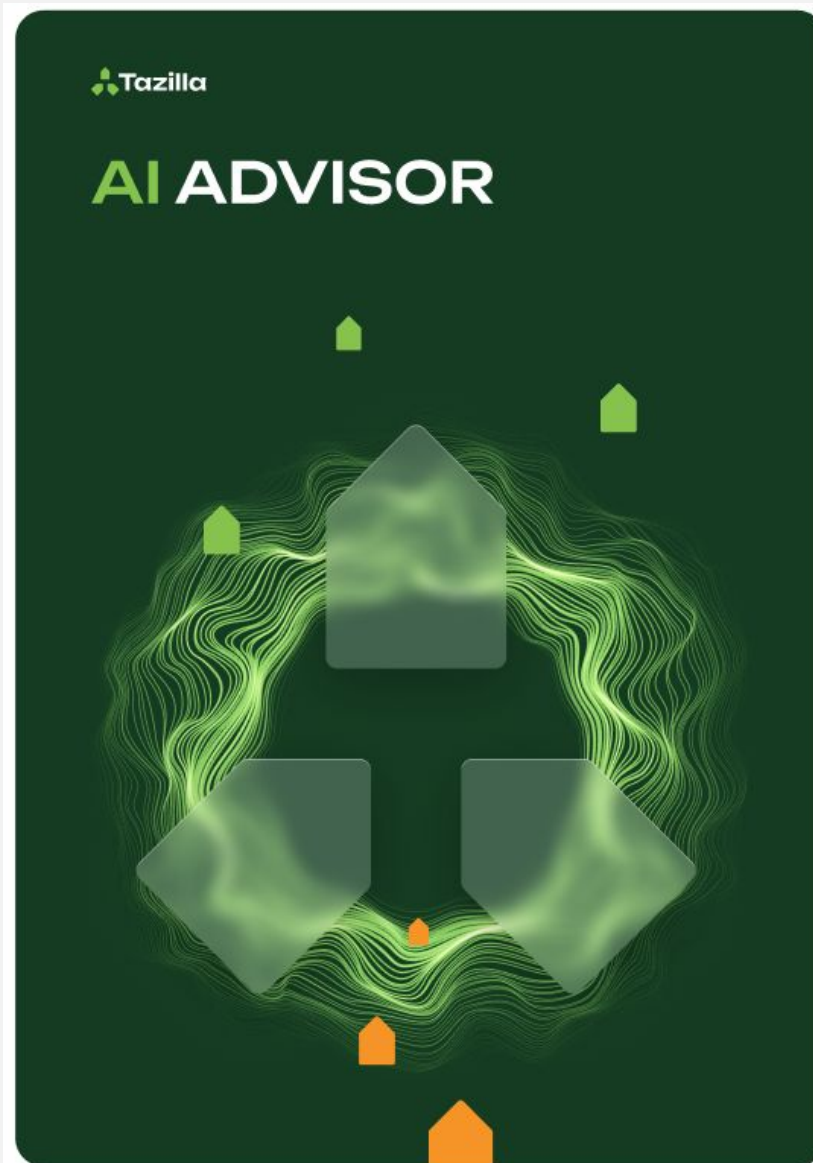
Phishing test

AI onboarding

AI zistí voľne dostupné údaje z internetu

Vyplní prázdny profil

Ušetrí čas používateľovi



[AI Advisor](#) [Services](#) [Impacts](#) [+ 4 more](#)

AI Content Creator

This AI-assisted wizard provides a **simplified interface for generating structured cybersecurity content and initializing key elements** of risk analysis. It serves both as a quick-start tool for creating context-aware baseline data tailored to your organization, and as a guided walkthrough of the essential steps required to complete a comprehensive risk assessment within the system.

By continuing, you acknowledge that this wizard uses AI-generated suggestions to support your cybersecurity risk analysis. The output is non-binding and should be reviewed before acceptance. By proceeding, you agree to the terms and conditions outlined in our [AI Usage and Privacy Policy](#).

Let's begin.

Organisation website

Risk analysis already in progress

You have an ongoing risk analysis.

Continue will guide you through the steps again so you can review, adjust, and continue where you left off.

Start New will clear your current work in progress (including workshops) and begin a fresh analysis.

[Back to dashboard](#)

[Start New](#)

[Continue](#)

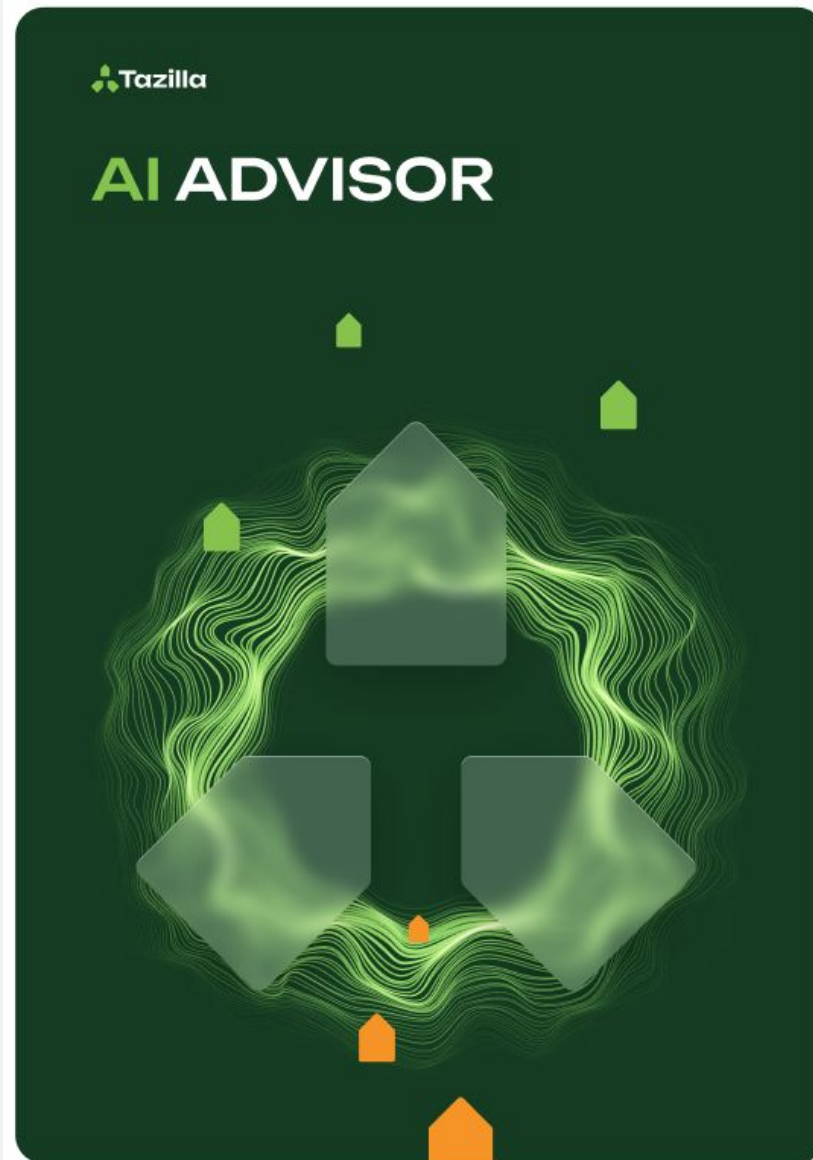
AI analýza rizík

Analýza rizík „je rocket science“



AI analýza rizík

Preto ju s AI spravíme na
mieru pomocou verejných
info



[AI Advisor](#) [Services](#) [Impacts](#) [+ 4 more](#)

AI Content Creator

This AI-assisted wizard provides a **simplified interface for generating structured cybersecurity content and initializing key elements** of risk analysis. It serves both as a quick-start tool for creating context-aware baseline data tailored to your organization, and as a guided walkthrough of the essential steps required to complete a comprehensive risk assessment within the system.

By continuing, you acknowledge that this wizard uses AI-generated suggestions to support your cybersecurity risk analysis. The output is non-binding and should be reviewed before acceptance. By proceeding, you agree to the terms and conditions outlined in our [AI Usage and Privacy Policy](#).

Let's begin.

Organisation website

Risk analysis already in progress

You have an ongoing risk analysis.

Continue will guide you through the steps again so you can review, adjust, and continue where you left off.

Start New will clear your current work in progress (including workshops) and begin a fresh analysis.

[Back to dashboard](#)

[Start New](#)

[Continue](#)

AI analýza rizík

Preto ju s AI spravíme na
mieru pomocou verejných
info



AI Content Creator

Core Business Services

Assets

AI Content Creator

This AI-assisted wizard provides a **simplified interface for generating structured cybersecurity content and initializing key elements** of risk analysis. It serves both as a quick-start tool for creating context-aware baseline data tailored to your organization, and as a guided walkthrough of the essential steps required to complete a comprehensive risk assessment within the system.

By continuing, you acknowledge that this wizard uses AI-generated suggestions to support your cybersecurity risk analysis. The output is non-binding and should be reviewed before acceptance. By proceeding, you agree to the terms and conditions outlined in our [AI Usage and Privacy Policy](#).

Let's begin. Just fill in the required information to get started.

Organisation website

www.google.com

Back to dashboard

Working



Ďakujem, **Peter Veľký** Práve analyzujem organizácie Google a pripravil vhodné nastavenia.

Organizáciu som si zaznamenal, teraz nastavujem jazyk prístupný na **Slovenčinu**.

Describe how you want the AI to adjust the content.. Number of assets

what are the biggest problems in cybersecurity for SME's right now?

Here are some of the **biggest cybersecurity problems** facing small and medium-sized enterprises (SMEs) right now (2025) — plus notes on *why* they're issues and some pointers for mitigation. Since you're working with SMEs (albeit in accessories / e-commerce) this should help frame your thinking.

1. Limited resources + lack of specialised expertise

- Many SMEs simply don't have the budget or staff to build an in-house security team, monitor 24/7, or stay on top of evolving threats. SCIRP +2
- They may also lack awareness or cybersecurity literacy: what threats exist, how to detect, how to respond. arXiv
- Because of that, SMEs often are easier targets for attackers (less "hardening"). NCX Group
Why it matters: If your business is digitally active (webshop, payment integration, cloud infrastructure) these limitations create gaps attackers can exploit.

Pointers: Prioritise core controls (patching, backups, strong passwords, multi-factor authentication), consider outsourcing to a managed service for security monitoring, allocate budget for regular training / awareness for your staff.

2. Phishing, social engineering & human error

- Phishing remains one of the top entry vectors for attackers targeting SMEs. Cyber Tech Guar... +2
- Human error (clicking malicious link, weak password, mis-configured cloud share) remains a big vulnerability. IT Pro +1
Why it matters: Regardless of how good your technology is, if people are not trained or aware, attackers will exploit that "weak link".

Pointers: Run basic training with your team (even small team), phishing-simulations (if possible), enforce MFA for all key systems, adopt principle of least privilege (so a single error doesn't lead to full compromise).

3. Ransomware & extortion-type attacks

5. Supply-chain, third-party & vendor risks

- SMEs may not only be targets themselves, they also may be weaker links in the supply chain of larger organisations. Attacks through third-party vendors or software dependencies are rising. securityexception... +1
Why it matters: Even if your systems are relatively secure, if you integrate with or depend on other vendors/suppliers who are not, you may still get compromised via them.

Pointers: Evaluate your vendors: their security practices, what access they have to your systems/data. Limit vendor permissions to "just enough". Include security clauses in vendor contracts. Monitor vendor access.

6. Lack of incident-response preparedness & resilience

- Many SMEs do not have formal incident-response plans, lack testing of backup/restoration, or lack continuity planning. IT Pro +1
Why it matters: If you *are* breached, your ability to respond, recover, restore operations will determine how much damage you suffer.

Pointers: Create a basic incident response plan (who does what when you detect a breach), perform tabletop exercises even informally, ensure you know how you'll communicate (internally + externally), know which backups you'll restore and how.

7. Evolving / sophisticated threats (AI-powered, targeted)

- Attackers are adopting more advanced tactics: AI-driven phishing, highly-targeted attacks, etc. WardenShield +1

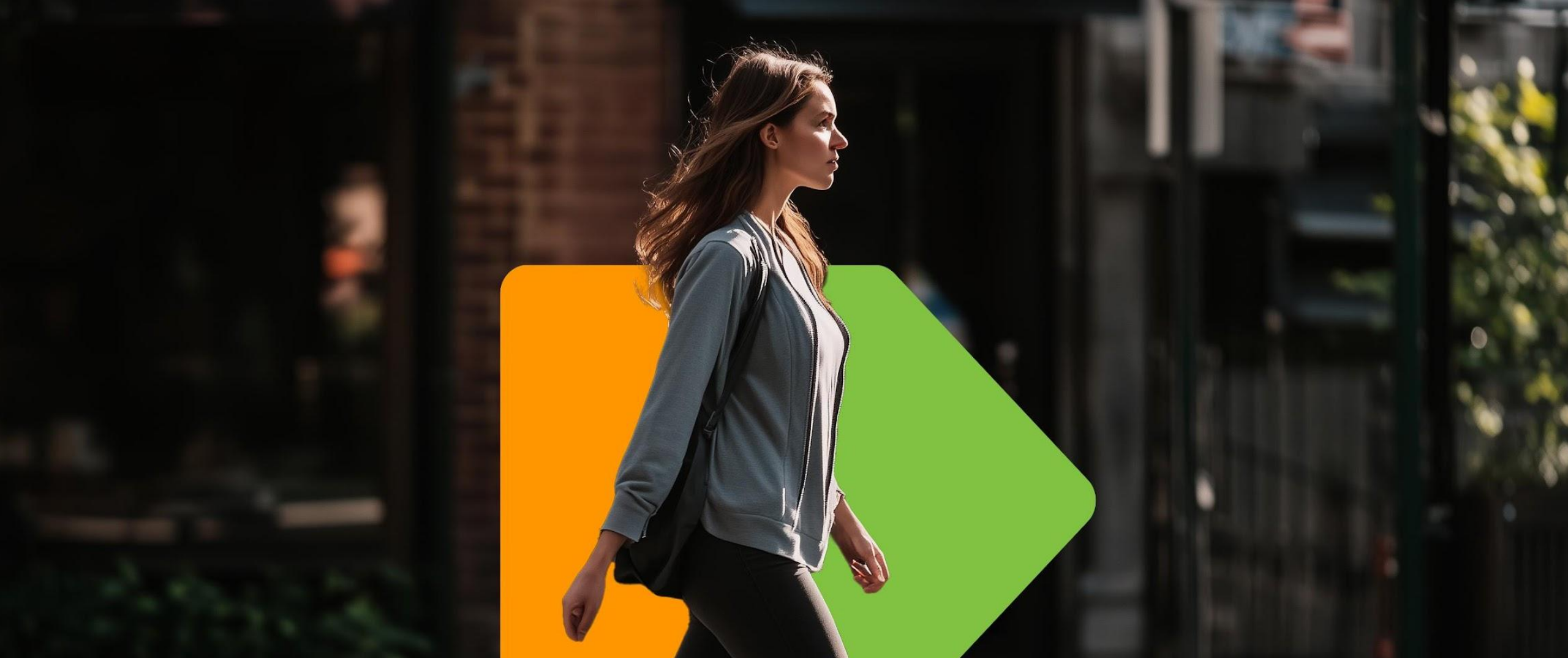
Why it matters: What used to be low-hanging fruit is evolving. If you assume "we're too small to be noticed", that's a dangerous mindset.

Pointers: Stay up to date with threat intelligence at least at a high level, ensure you have layers of defence (not just one security control), consider adopting "detect and respond" mindset not just "prevent".

8. Regulatory/compliance burdens & business risk awareness

- In many jurisdictions (especially EU) SMEs are increasingly subject to regulations (data protection, breach reporting, etc). Also cybersecurity is a **business risk** (not just an IT issue) — leadership awareness is still often lacking. The Times +1
Why it matters: If you treat cybersecurity only as "IT's job", you may miss bigger business-impact issues: e.g., reputational damage, customer trust, supply-chain compliance, liability.

Pointers: Elevate cybersecurity to board/leadership level (even if small business) — ensure someone is accountable; consider including it in your risk-register; keep abreast of regulatory obligations (breach notification, minimum security controls, etc).



Financovaný
Európskou úniou

www.tazilla.com

Beta verzia zdarma do 04/2026

