Why Small Businesses Don't Take Security Seriously

And how to fix that with 3 simple shifts

1


Common Objections to Cybersecurity
Small businesses often have misconceptions that prevent them from investing in proper security measures.
"We're too small to be a target."
"Security is too expensive/complex."
"We don't have anything valuable to steal."
"It won't happen to us."

2

THE DISCONNECT

Communication Breakdown

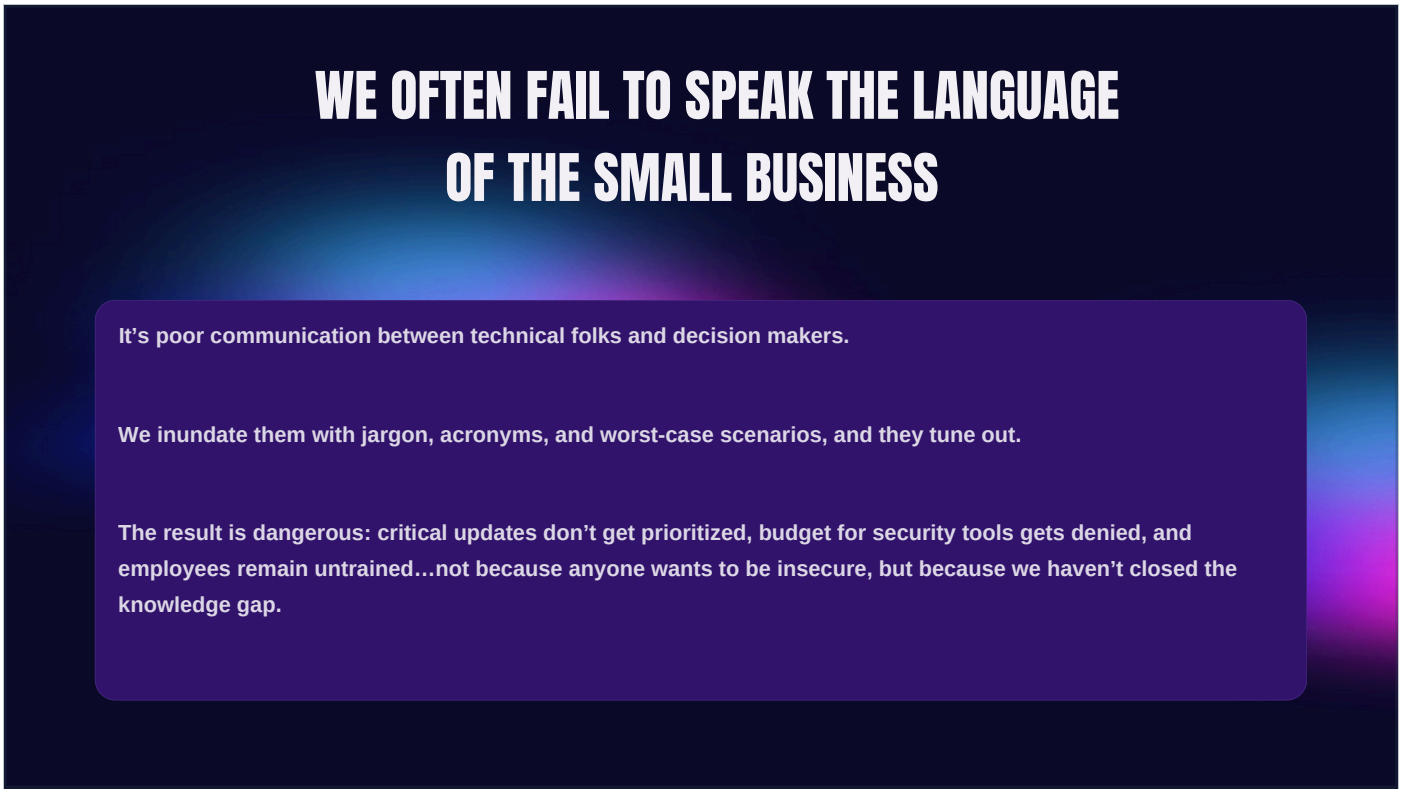
It often comes down to a mindset gap and communication failure.

Business owners aren’t inherently reckless… rather, many simply don’t understand the technical threats or see how those threats translate into business risks.

They’ve never had cybersecurity explained in plain English that connects to their world.

The owner just hears technical gobbledygook

3


WE OFTEN FAIL TO SPEAK THE LANGUAGE
OF THE SMALL BUSINESS
It’s poor communication between technical folks and decision makers.
We inundate them with jargon, acronyms, and worst-case scenarios, and they tune out.
The result is dangerous: critical updates don’t get prioritized, budget for security tools gets denied, and employees remain untrained…not because anyone wants to be insecure, but because we haven’t closed the knowledge gap.

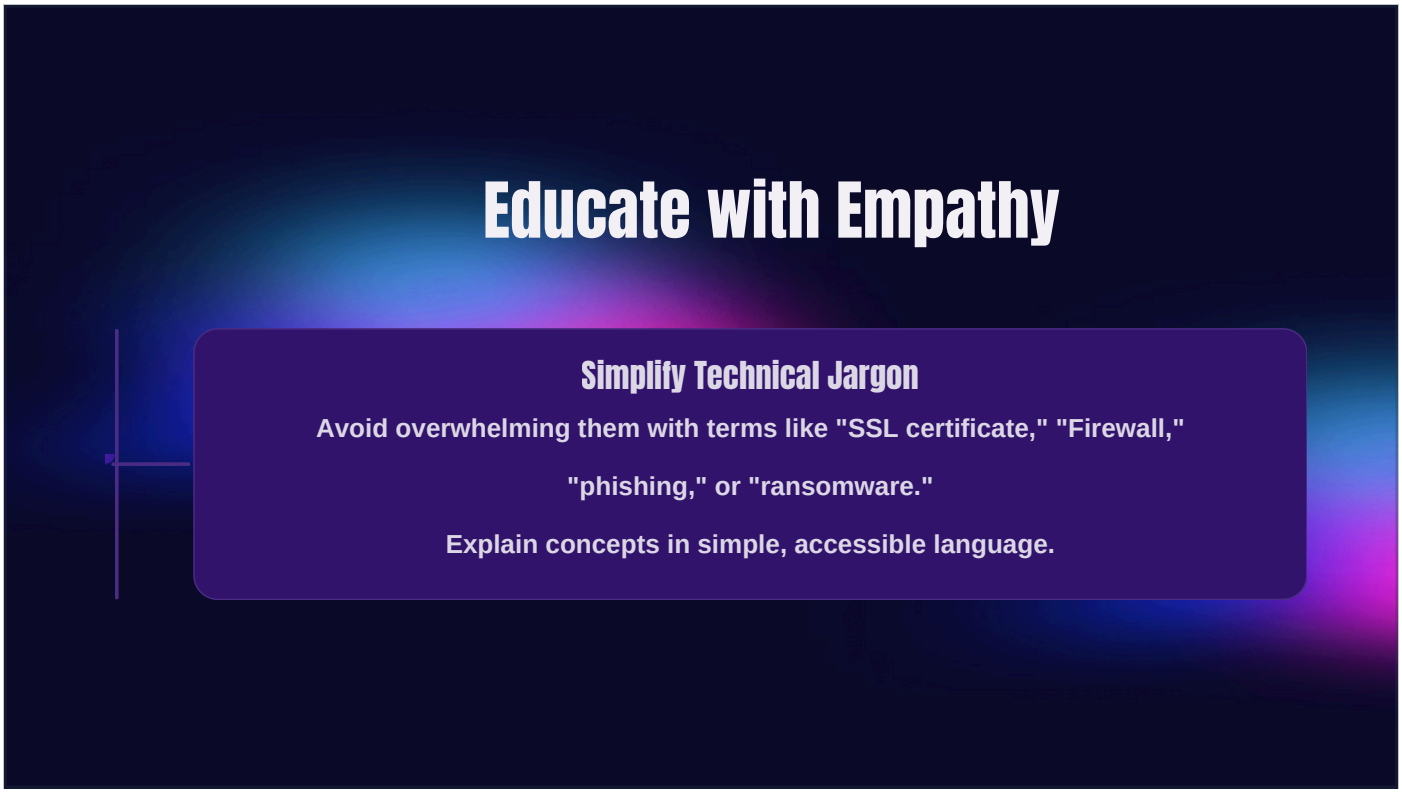
4

5


IT REQUIRES Three Fundamental Shifts
BRIDGE the Communication Gap
Make cybersecurity understandable and relevant to non-tech people
Reframe Security as Business Asset RATHER THAN A HURDLE
Position security as something that enables trust and growth
Provide Practical Framework..
(Non Intimidating)
Build good security habits step by step without overwhelming small teams

6

The biggest security risk isn’t just bad code or zero-day exploits – it’s the communication breakdown between tech professionals and business stakeholders. If we can’t effectively communicate risks and solutions to small-business owners, nothing will change. As security experts or developers, we need to step out of our technical bubble and meet our audience where they are. This means translating geek-speak into plain language and framing security in terms that owners and managers care about.
7


Educate with Empathy
Simplify Technical Jargon
Avoid overwhelming them with terms like "SSL certificate," "Firewall," "phishing," or "ransomware."
Explain concepts in simple, accessible language.

8


Analogies Help Demystify Abstract Concepts
Use Analogies from Everyday Business Life (Relatable)

9


BEFORE 👉 AFTER
"You need multi-factor authentication across your systems."
"Your password gets you to the door, but MFA is the security guard that checks your ID."
"We need to apply the latest security patches to your environment."
"Updates are like changing the locks after you lose your keys. Hackers already know how to pick the old ones."
"An unpatched system is like leaving a broken window unfixed ... it looks harmless until it rains."
"We'll implement a multi-phase cybersecurity maturity model."
"We'll start small and scale up. Crawl → Walk → Run.At crawl, it's basics like passwords and updates.At walk, it's policies and backups.At run, it's advanced tools once you've built habits."
"OpenSSL is a widely used open-source toolkit for SSL and TLS protocols that ensure encrypted communication."
"OpenSSL is the technology that protects nearly two-thirds of all websites online..it's like the internet's security guard. Every time someone checks out, signs in, or shares information, OpenSSL makes sure no one's eavesdropping."

10

If an owner asks

“Why would anyone target me?

I’m just a local shop,” don’t scoff.. explain that hackers often target small firms because they know security is weaker

(“just like a burglar choosing the house

with an open window”)

11

61% of small businesses

were targeted by cyberattacks in one year 2024 (not all successful). Hackers count on small companies being unprepared.

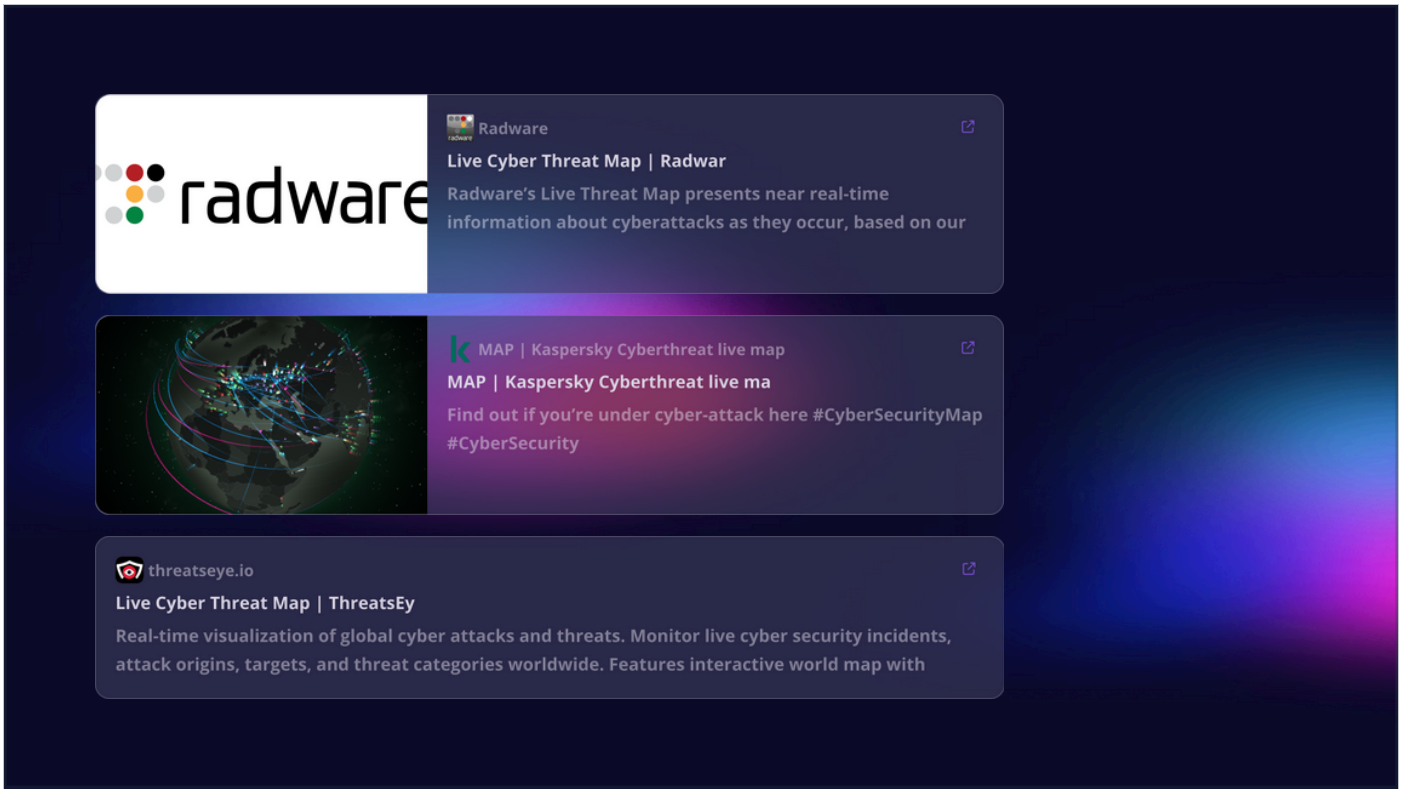
Each small business might yield a modest ransom or payout, but those payouts add up. Ransomware gangs and phishing crews increasingly operate on a “quantity over quality” model

It’s often more profitable to extort 100 small companies for $5,000 each than to score one $500,000 heist and it carries less risk for the criminals

THIS CAN BE AN EYE OPENER

12

13


radware
Radware
Live Cyber Threat Map | Radwar
Radware's Live Threat Map presents near real-time information about cyberattacks as they occur, based on our
MAP | Kaspersky Cyberthreat live map
MAP | Kaspersky Cyberthreat live ma
Find out if you're under cyber-attack here #CyberSecurityMap #CyberSecurity
threatseye.io
Live Cyber Threat Map | ThreatsEy
Real-time visualization of global cyber attacks and threats. Monitor live cyber security incidents, attack origins, targets, and threat categories worldwide. Features interactive world map with

14

Real-World Impact: Rokenbok Education

A 7-employee toy company "realized its worst nightmare" when hackers froze their database with ransomware during holiday season. Four frantic days to rebuild systems, untold lost sales.

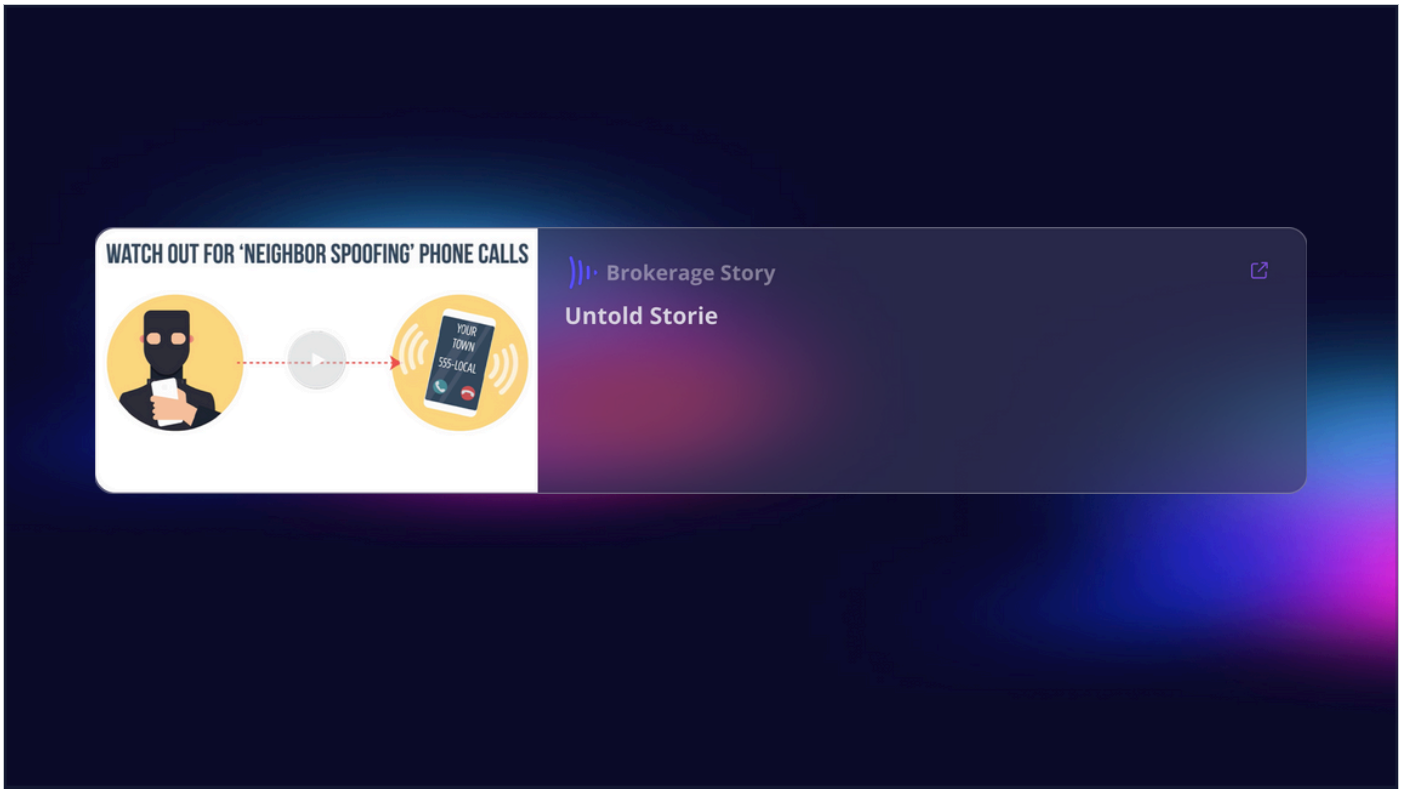
Stories like this make threats real and show lessons: not every small business recovers.

By sharing such examples, you're not just saying "this could happen," you're showing it already happened to someone like you. That can be hugely persuasive.

Share examples similar to your target audience which will help shorten the sales cycle.

15

16


WATCH OUT FOR 'NEIGHBOR SPOOFING' PHONE CALLS
YOUR TOWN 555-LOCAL
Brokerage Story
Untold Storie

17

Communicate Positive Outcomes, Not Just Fear

The Pitfall of Fear-Based Messaging

Constantly telling scary breach stories can backfire. Owners may feel overwhelmed or conclude, "If disaster is inevitable, why try?" This can lead to apathy and inaction.

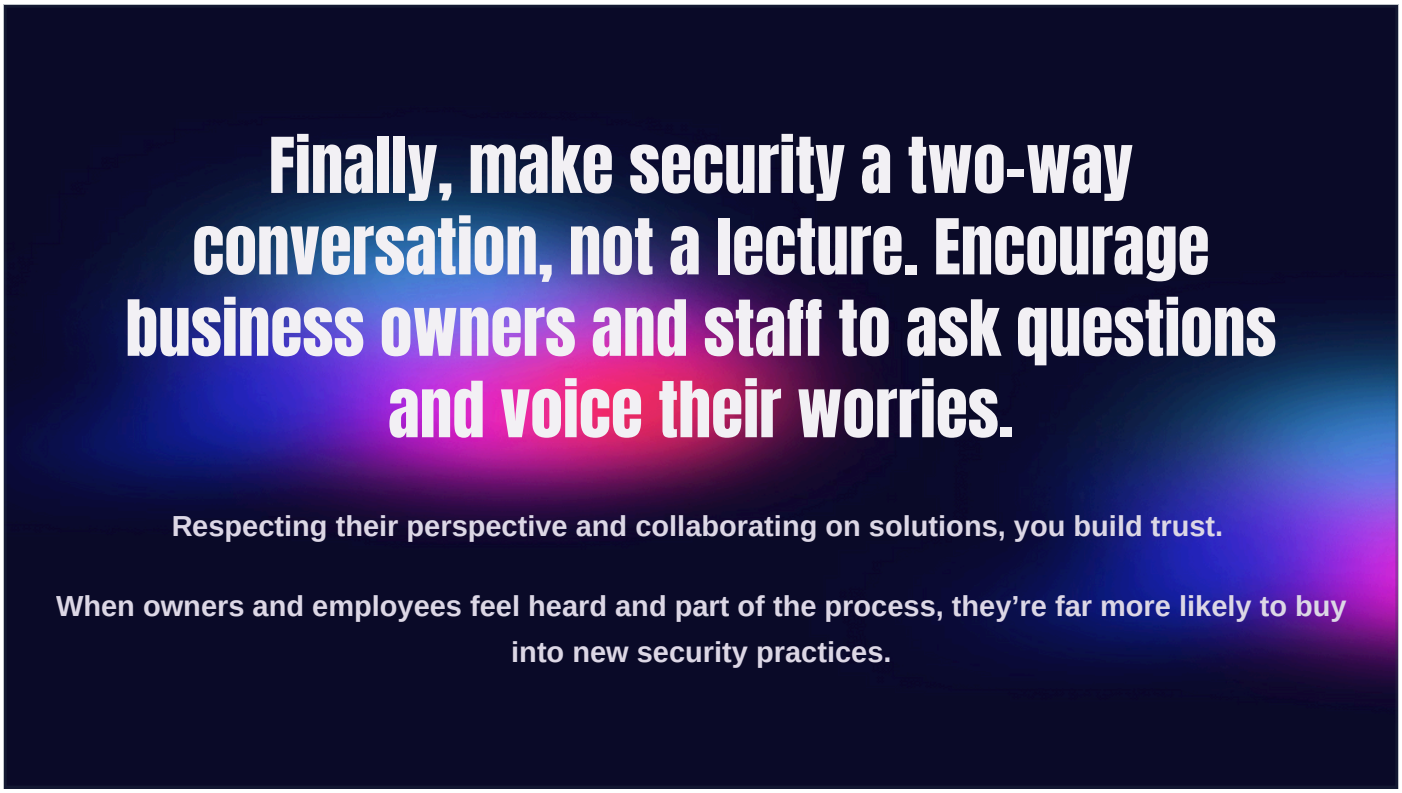
Balance the Narrative

Instead, emphasize that preventative steps work and are manageable. Highlight successes and the effectiveness of proactive measures, fostering a sense of empowerment.

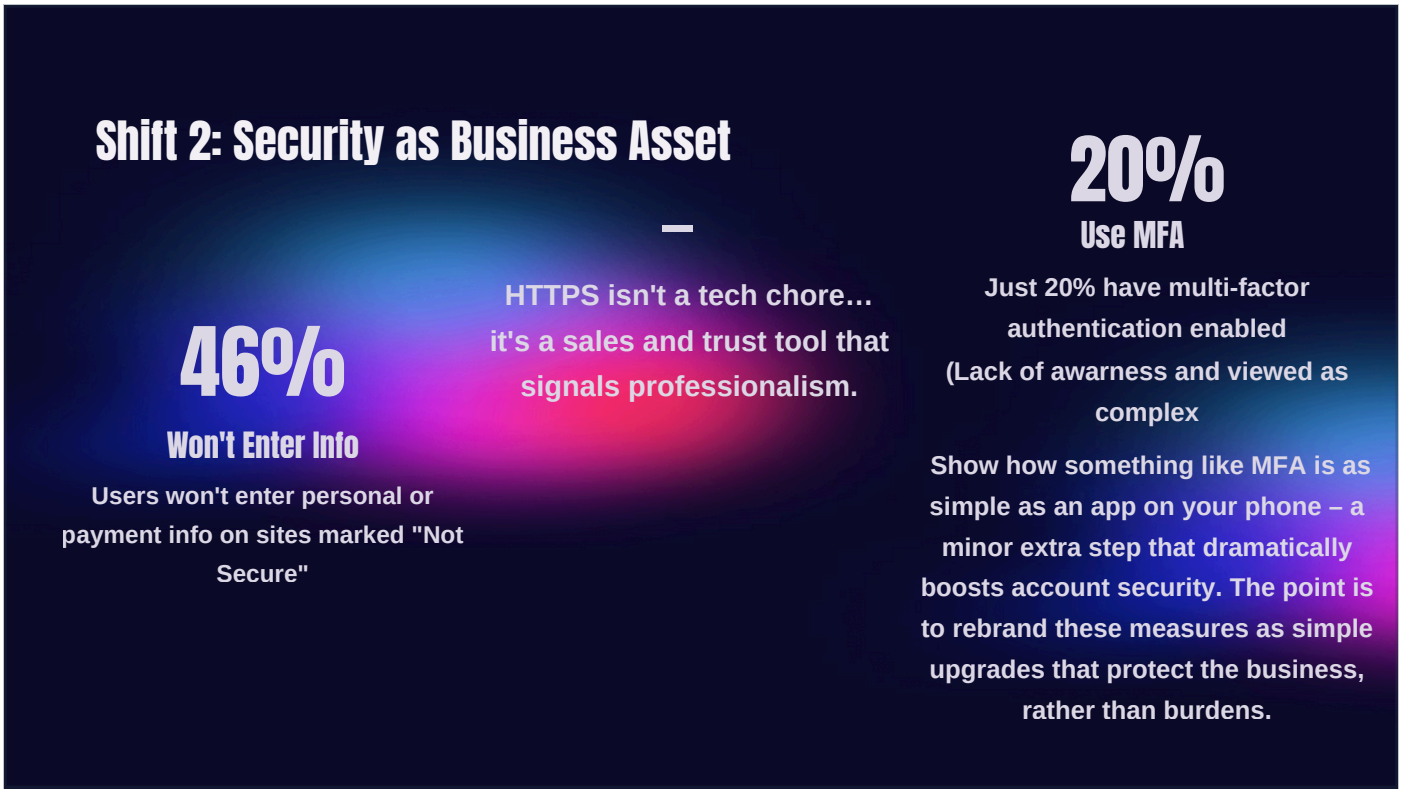
Actionable Prevention

For example: "Just by training your staff to spot phishing emails, you can cut the biggest risk of a hack. Most attacks, even at small businesses, start with an employee being tricked." Emphasize simple, impactful steps.

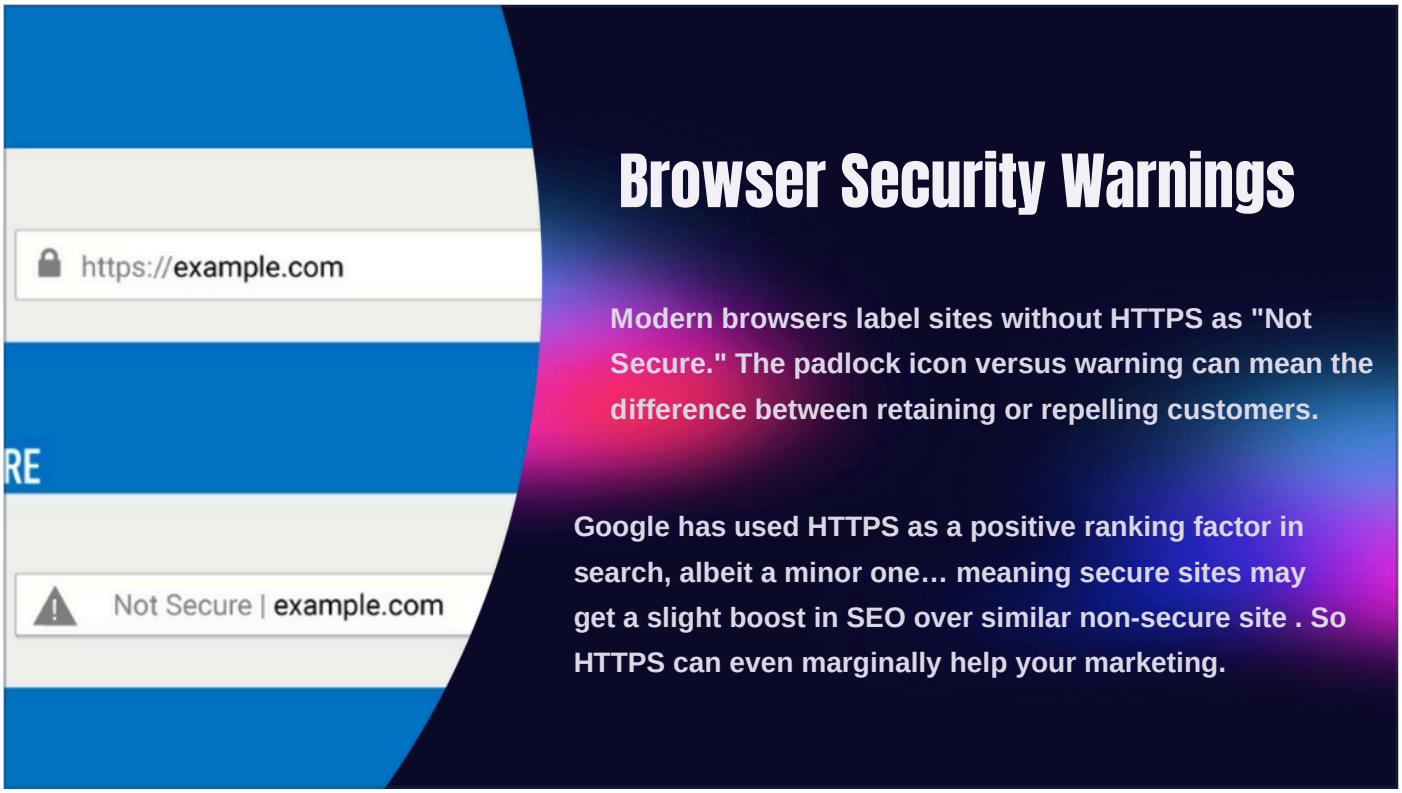
18


Finally, make security a two-way conversation, not a lecture. Encourage business owners and staff to ask questions and voice their worries.
Respecting their perspective and collaborating on solutions, you build trust.
When owners and employees feel heard and part of the process, they’re far more likely to buy into new security practices.

19


Shift 2: Security as Business Asset
46%
Won't Enter Info
Users won't enter personal or payment info on sites marked "Not Secure"
HTTPS isn't a tech chore… it's a sales and trust tool that signals professionalism.
20%
Use MFA
Just 20% have multi-factor authentication enabled
(Lack of awarness and viewed as complex
Show how something like MFA is as simple as an app on your phone – a minor extra step that dramatically boosts account security. The point is to rebrand these measures as simple upgrades that protect the business, rather than burdens.

21


https://example.com
RE
Not Secure | example.com
Browser Security Warnings
Modern browsers label sites without HTTPS as "Not Secure." The padlock icon versus warning can mean the difference between retaining or repelling customers.
Google has used HTTPS as a positive ranking factor in search, albeit a minor one… meaning secure sites may get a slight boost in SEO over similar non-secure site . So HTTPS can even marginally help your marketing.

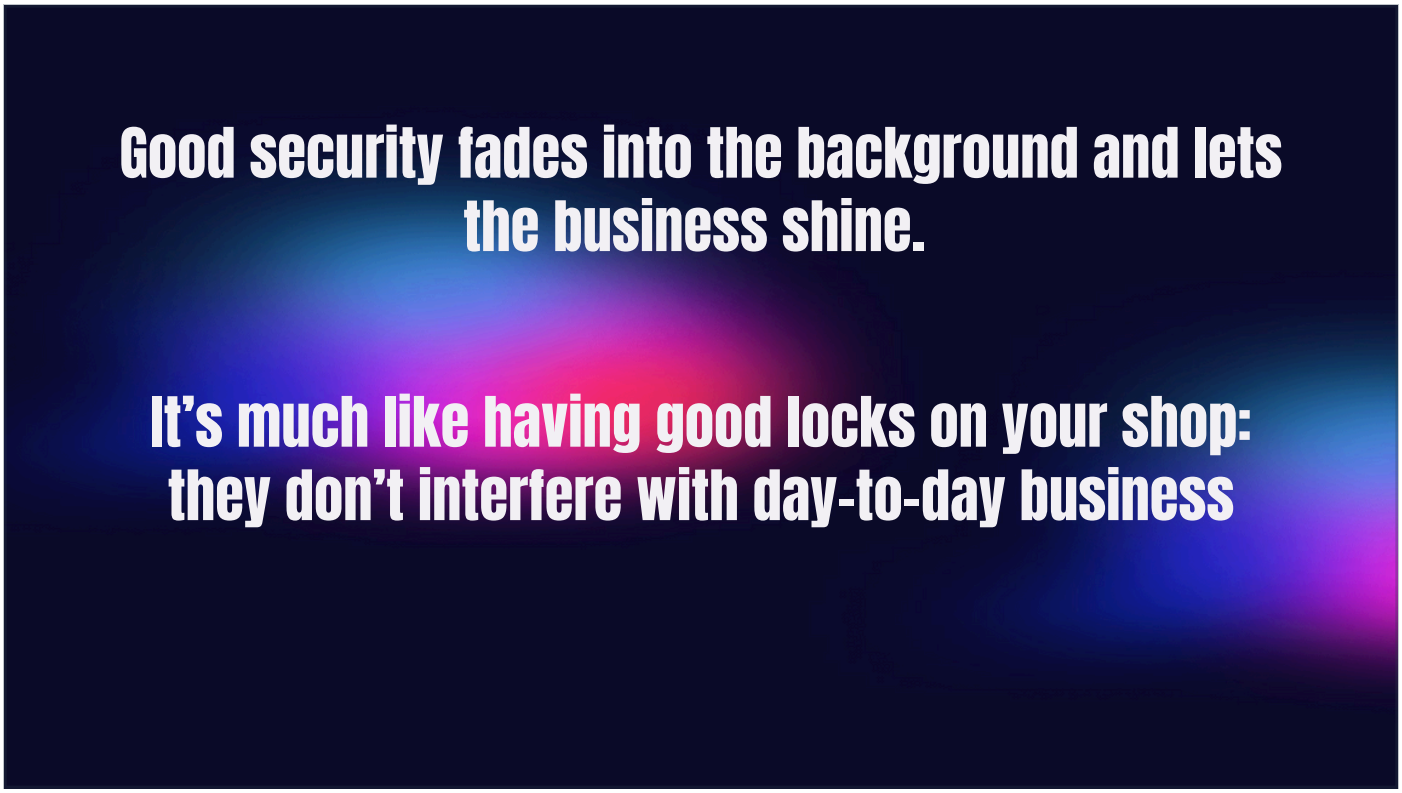
22


From Cost Center to Business Asset
Present encryption as a competitive advantage - it's about protPecting customers and assuring them "we take your data seriously." This shift in perspective turns a security measure into a selling point.
Security can also be positioned as a business enabler when working with larger partners or complying with laws.
"Opportunity for Bigger Contracts and Opportunities" B2G

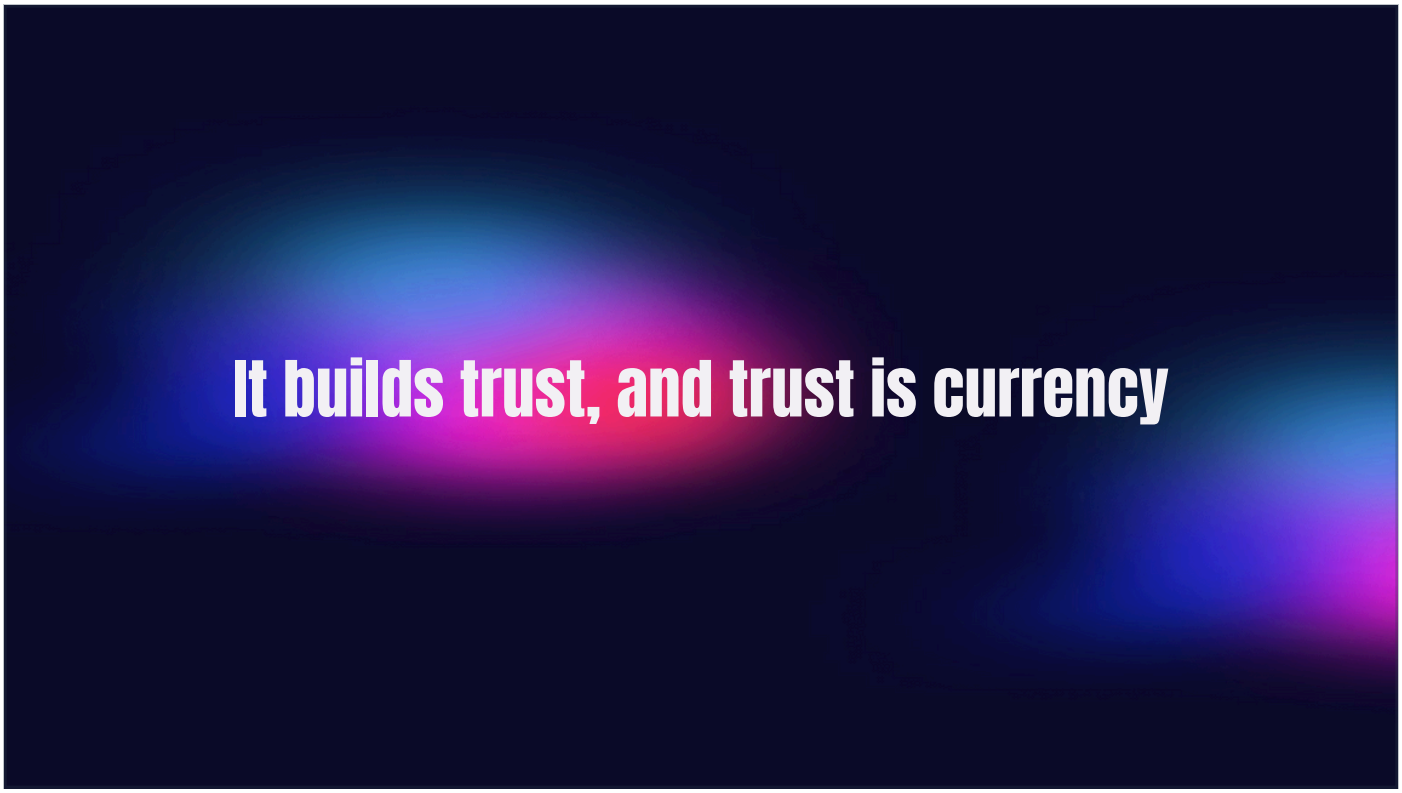
23


Addressing the perception that security is expensive, complex, and stifling
Many small-business folks fear that adding security will slow down their processes, require hiring expensive experts, or bury them in technical upkeep.
We have to dispel these myths by highlighting how far security tech has come in being user-friendly and cost-effective.

24


Good security fades into the background and lets the business shine.
It’s much like having good locks on your shop: they don’t interfere with day-to-day business

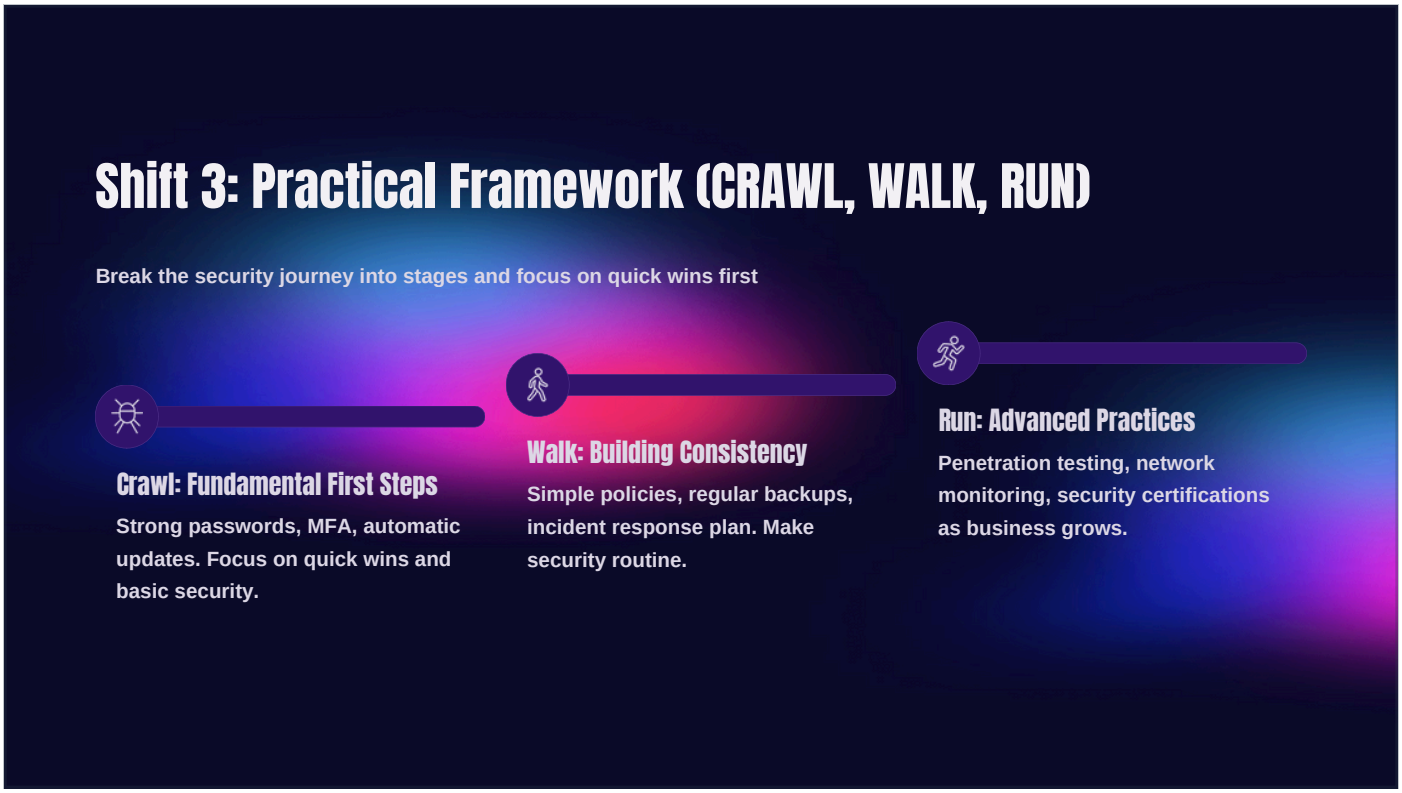
25



26


When small businesses start to see security
as a brand enhancer and growth enabler,
they'll be far more enthusiastic (and less resistant)
about embracing things like OpenSSL updates,
encryption tools, and other best practices.

27



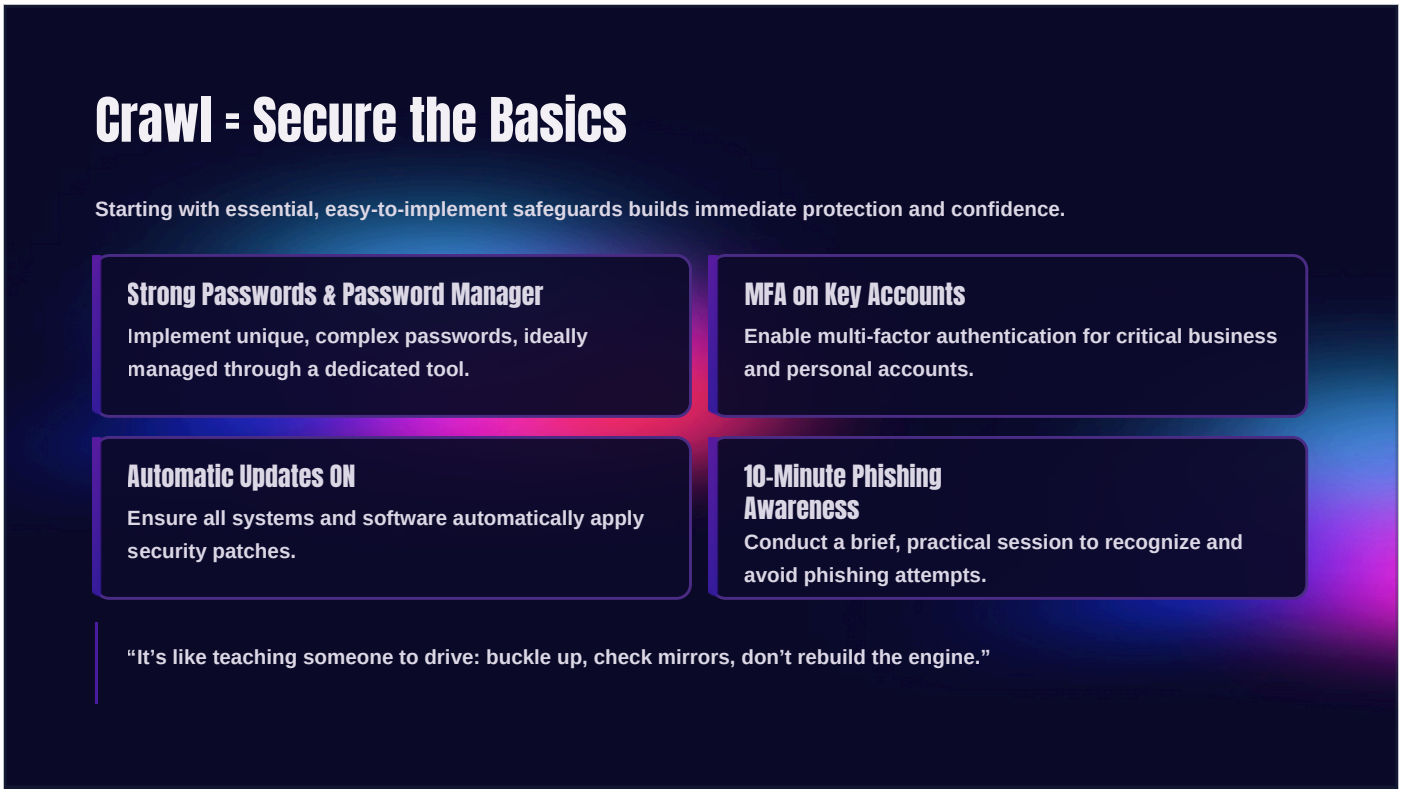
Crawl (Fundamental First Steps): Begin with a basic security hygiene check and tackle the most glaring risks. For a small business, this usually means addressing human factors and easy vulnerabilities first. For example, ensure the company is using strong, unique passwords (or better yet, a password manager) and enable multi-factor authentication on important accounts – since 80% of hacking incidents involve stolen or weak credentials strongdm.com . Set up automatic software updates on all systems, so critical patches (like those for OpenSSL or the operating system) are applied without relying on someone to remember. These steps are low-cost or free, and they provide huge bang-for buck in risk reduction. Also, train employees on the basics of phishing and safe browsing..not through hours-long lectures, but with a short, relatable session or even a fake phishing email test to see who clicks. The key at the "crawl" stage is simplicity. Give them a short checklist of must-dos, not an encyclopedia of security. s an analogy, it's like teaching a new driver: you start with "buckle your seatbelt, check your mirrors," not how to rebuild an engine. Quick wins build confidence. For instance, once they implement something like MFA and see it working, they'll feel more secure and be ready for the next step.

Walk (Building Consistency and Policies): After the fundamentals, move into establishing some consistent policies and backups. This might involve creating simple security policies for the team... for example, an acceptable use policy for work devices (don't install random apps, don't reuse work passwords elsewhere, etc.), and a clear process for handling sensitive data. Emphasize making these policies short and understandable – even a one-page "Top 5 Security Rules" poster can suffice at first. At this stage, also ensure they have regular data backups and a

basic incident response plan. A small business doesn't need an elaborate 50-page incident response plan, but they should know the basics of what to do if something goes wrong (e.g., who to call if systems are hacked or encrypted by ransomware, where backups are stored, how to communicate to customers if needed). Think of this as "walk" because it's about developing routine practices: maybe quarterly security meetings or trainings, scheduled software update reviews, etc. At this point, it's useful to introduce tools that make security easier. For example, use a managed antivirus/anti-malware service that updates automatically, or a cloud security dashboard if they have one (many SaaS tools for small biz now include security health checks). The idea is to integrate security into regular operations without it dominating their time. If you can, assign a security point-person or champion within the team (perhaps someone with an interest in tech) … not to make them a full on CISO, but to liaise with IT and keep an eye on things. This distributes responsibility a bit and empowers the team internally.

Run (Advanced Practices and Continuous Improvement): Once the basics are solid and part of routine, a small business can "run" by adopting more advanced or specialized security measures as needed. This could include things like penetration testing or hiring an external security consultant annually to probe their defenses. They might implement more sophisticated tools like network monitoring, or encrypted VPNs for remote access, if their business demands it. At this stage, they might also pursue security certifications or frameworks depending on their industry to formalize their security posture.

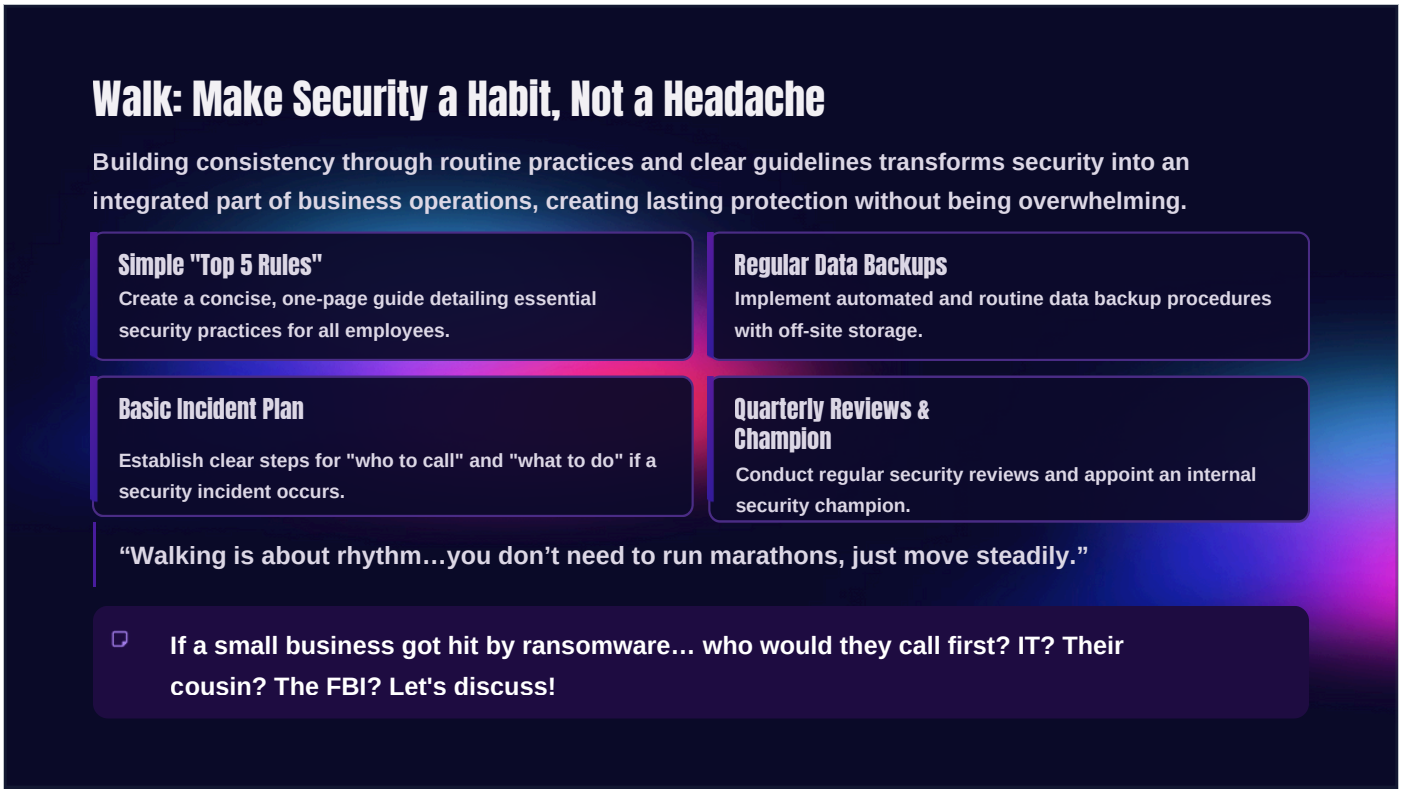
The "run" phase is all about scaling security in line with business growth. Perhaps by now the business has grown to where it can invest in a dedicated IT/security staff or managed security service. The important thing is, by this stage the company culture has embraced security as part of its DNA, thanks to the earlier groundwork. Employees are now used to annual refreshers or drills, just like they might be used to fire drills. Security becomes "business as usual."
28



"Crawl is all about momentum. You start with small, visible wins that make the owner feel, 'Hey, we can do this.'

We're not teaching them encryption algorithms ... we're showing them how to avoid clicking the fake invoice from 'Amazon Billing Department.'

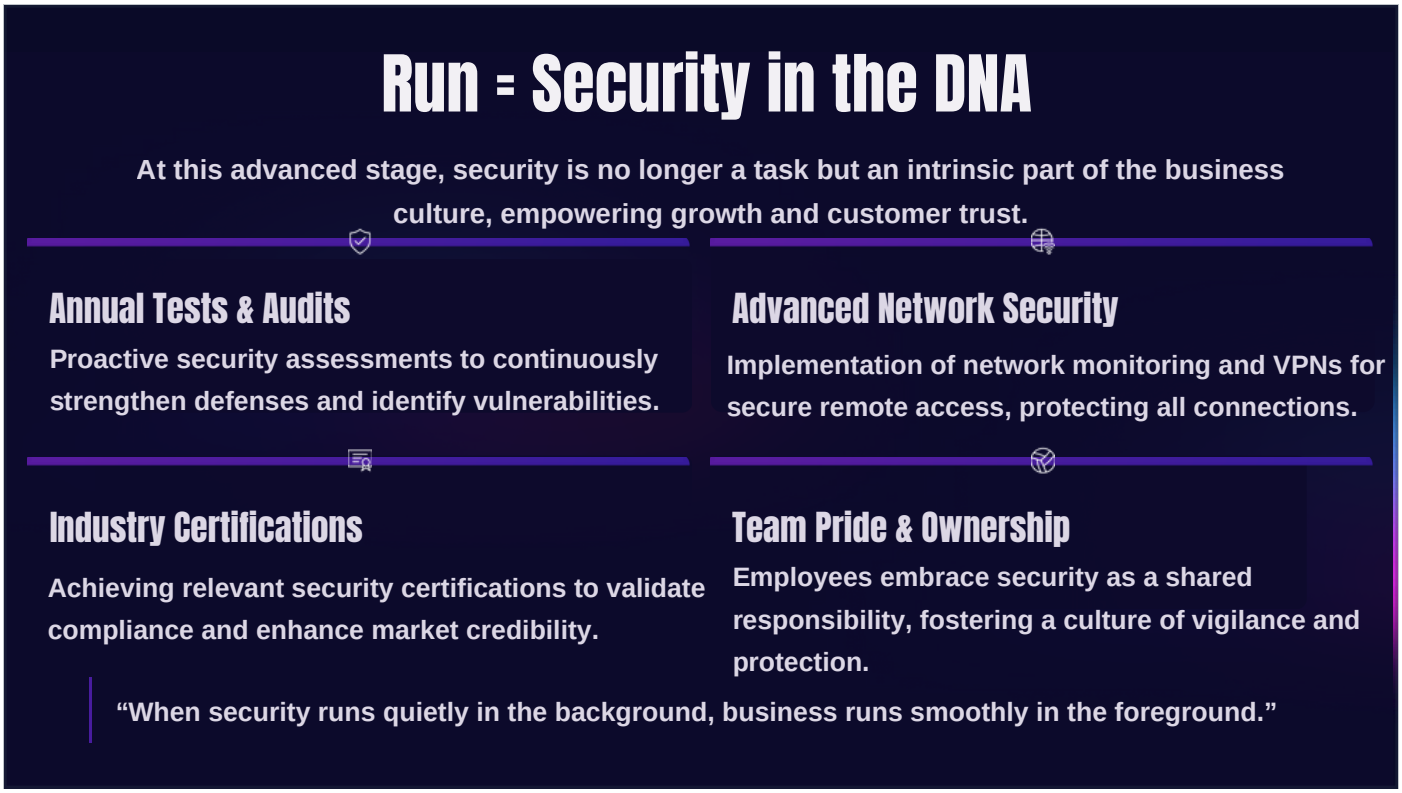
Quick wins build trust .. and trust builds buy-in."
29



“At Walk, security becomes muscle memory.

This is where we start to add small habits that repeat: weekly updates, quarterly reviews, and knowing who to call when something goes wrong.

You don’t need a 50-page policy. You need five clear rules taped to the office wall.”
30

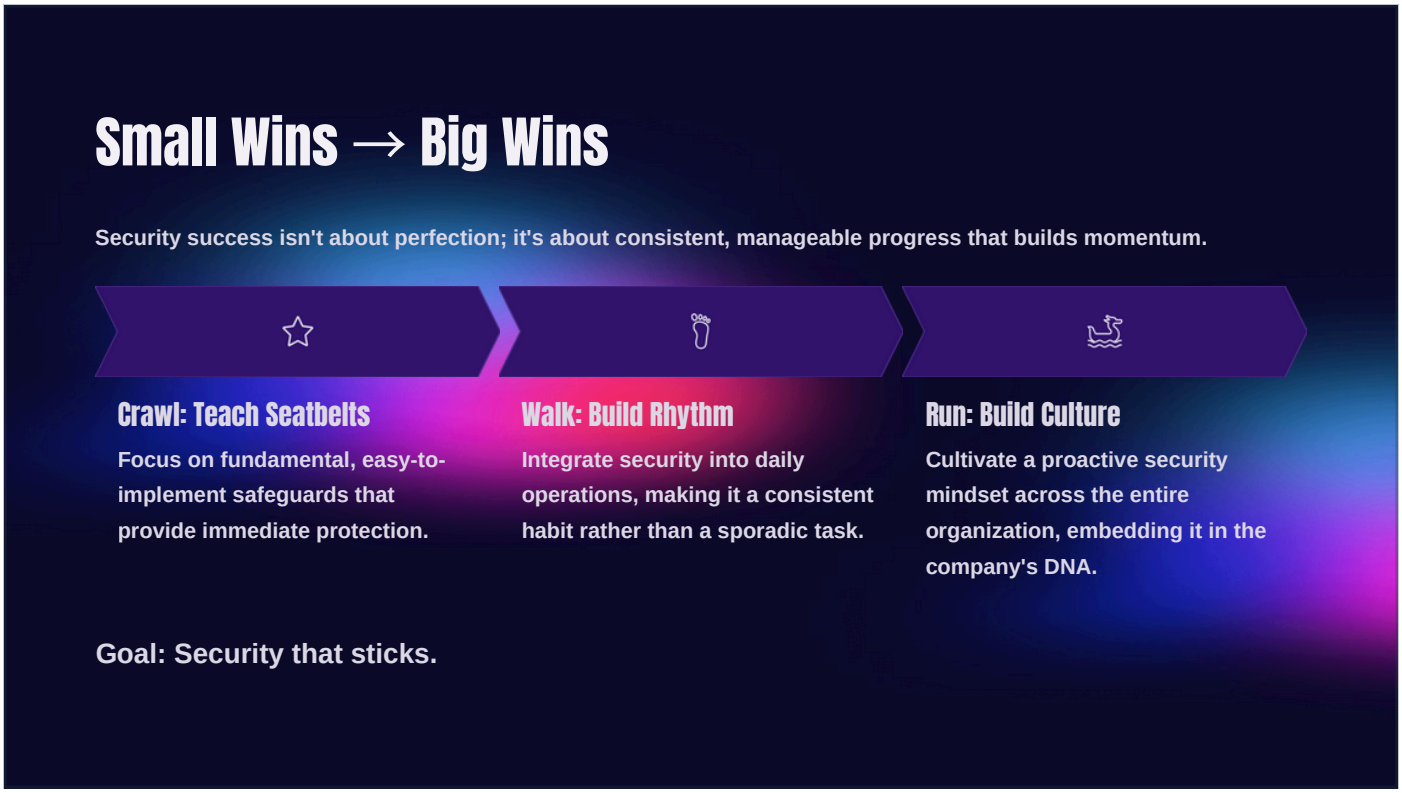


“Run is where small businesses stop seeing security as something they have to do and start seeing it as something they are proud to do.

They’re not checking boxes anymore they’re leading with confidence.”

“Think of a client you’ve helped mature from chaos to control .. what was their Run moment?

The moment you thought, ‘They get it now.’
31



“Most small businesses fail at security not because they don’t care — but because it feels overwhelming.

Your job isn’t to make them experts. Your job is to make them believe: ‘We can do this.’

If you get them to take the first step, they’ll take the next one.”

Ask: “Where do most small businesses you work with sit today — Crawl, Walk, or Run?”

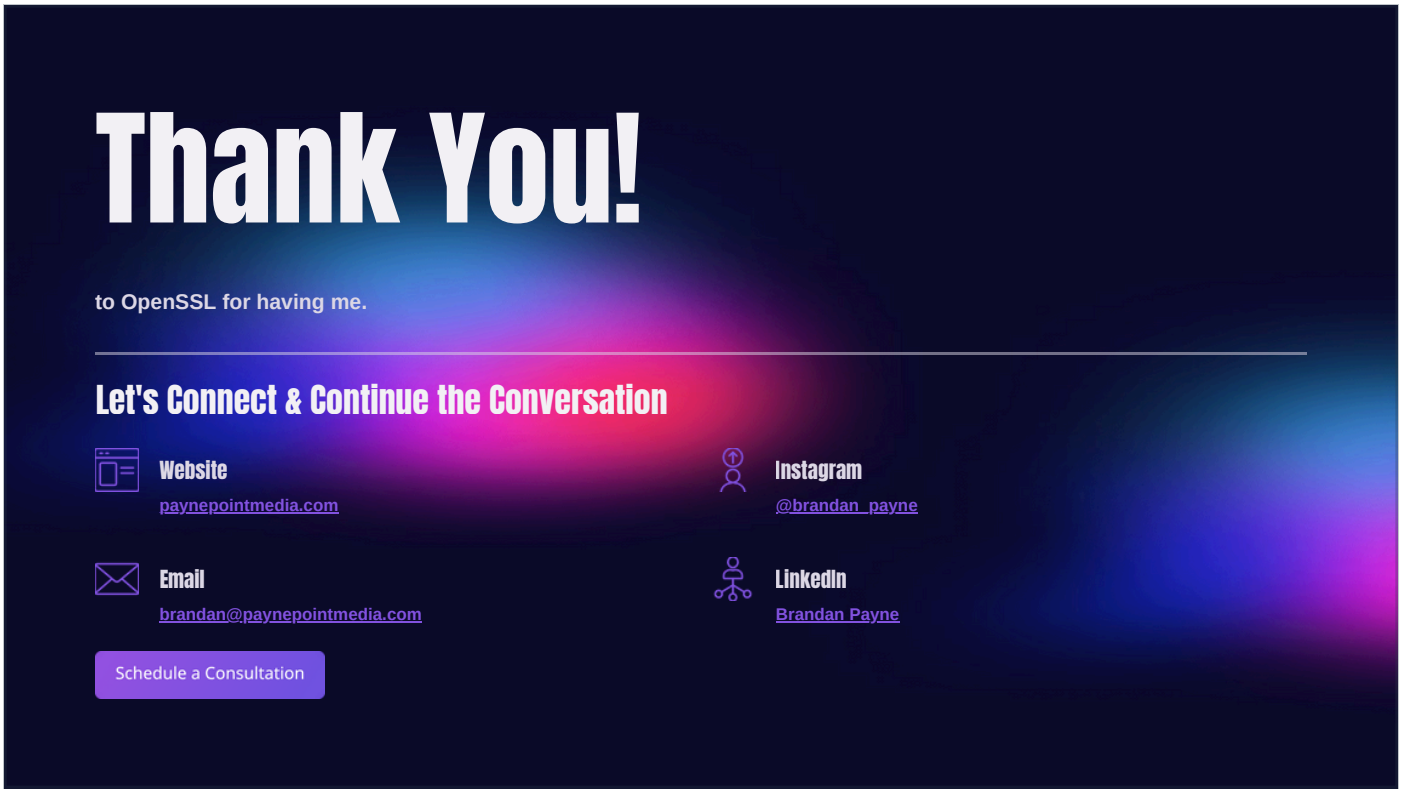
(Let hands raise; use humor. Then close strong:)
32


Small businesses are the backbone of our economy and communities.
They deserve world class security as much as any big corporation and with our help, they can achieve it.
It’s time to make cybersecurity not just a “big company thing,”

33

This slide is the culmination of the "how to fix the disconnect." It summarizes the core message: it's not about complex technical solutions but about human connection, clear communication, and building trust.

The "Teach in bites, not bytes" line is a play on words to emphasize practical, digestible advice.
34


Thank You!
to OpenSSL for having me.
Let's Connect & Continue the Conversation
Website
paynepointmedia.com
Instagram
@brandan_payne
Email
brandan@paynepointmedia.com
LinkedIn
Brandan Payne
Schedule a Consultation

35