SOLUTION BUILDERS®

BOOK THREE
THE RISE SERIES

RISE · S is for Secure

BUILT

Secure.

Why cybersecurity is the foundation every modern business stands on, and how a full framework keeps your momentum unbreakable.



R	I	S	E
Resilient	Integrated	Secure	Evolving

RISE · S is for Secure

Security is not a feature you bolt on later. It is the floor everything stands on.

Picture your business like a team on a winning streak. Every project shipped, every client won, every quarter beaten, that is momentum, and momentum is the most valuable thing you have. Now picture the one hit that ends a season in a single afternoon. In sport it is an injury. In business it is a breach. It freezes operations, drains cash, shatters trust, and in the worst cases it closes the doors for good.

Here is the part most people miss. The companies that get hit hardest are rarely the ones with the weakest tools. They are the ones who treated security as a project with an end date, a thing you buy once and forget. Real security is not a product. It is a **framework**, built into the foundation and woven through everything above it. That is exactly what the **S in RISE** stands for, and it is why we put it at the center.

R	I	S	E
Resilient	**Integrated**	**Secure**	**Evolving**
Cloud, continuity, backup	Infrastructure, services	Cybersecurity	AI

What you will take away from this book

Four chapters, one promise. By the last page you will understand why a secure foundation comes first, how a layered framework actually works, why testing your defenses matters as much as building them, and how your own people become your strongest wall. **Practical, visual, and built to be read, not skimmed.**

INSIDE THIS BOOK

Four chapters, one secure foundation.

01 The Foundation

Why a breach is the one thing that stops momentum cold, what it really costs, and how an attack actually unfolds.

- The momentum curve
- The true cost of a breach
- Anatomy of an attack

02 Harden Every Layer

Defense in depth, from endpoints to identity. The difference between legacy antivirus, EDR, and a managed team that never sleeps.

- Defense in depth
- Antivirus vs EDR vs MDR
- Backup and recovery
- A $100M lesson from Pixar

03 Test It Before They Do

Pen testing and breach simulation. Finding the cracks on your terms, and the maturity ladder that shows where you stand.

- The testing loop
- Scan vs test vs simulate
- The maturity ladder

04 Your People Are The Perimeter

The human firewall. Why most breaches are invited in, and how training flips your team from weakest link to strongest defense.

- The human element
- Social engineering decoded
- Building the human firewall

CHAPTER 01

SECURE · THE RISE SERIES

01

The Foundation.

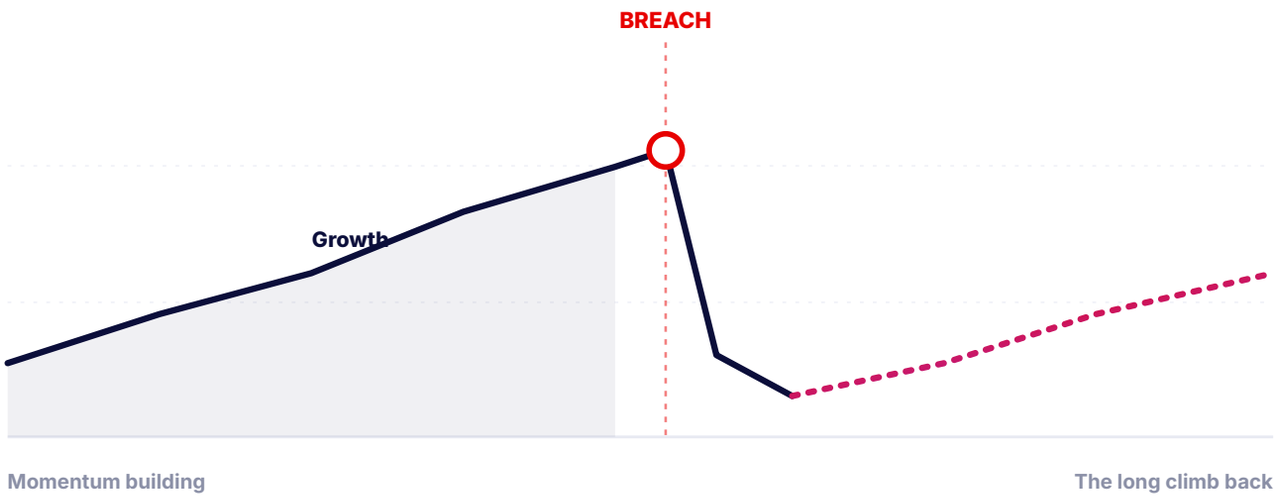
One breach can do what no competitor ever could, stop your business in its tracks. Before you build anything, you build the thing that keeps it all standing.

A breach does not just cost money. It costs your momentum.

Growth compounds. So does damage. A single incident can erase months of progress in an afternoon, and the climb back is always slower than the fall. Worse, the costs you can see, the ransom, the recovery, are only the surface. Underneath sit the quiet killers, lost customers, a damaged reputation, and a team pulled off the work that drives the business forward.

The momentum curve

ILLUSTRATIVE



$4.44M

Global average cost of a single data breach

IBM Cost of a Data Breach 2025

241

Average days just to identify and contain a breach

IBM 2025

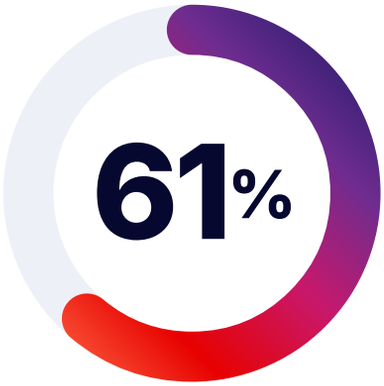
$3.31M

Average breach cost for companies under 500 staff

IBM 2025

Smaller does not mean safer. It often means targeted.

Attackers go where the doors are easiest to open. Growing companies hold valuable data but rarely have a full time security team watching it, and that gap is exactly what gets exploited.



of small and midsize businesses reported a breach in the past year

PreVeil, 2025

43% of all cyberattacks aim squarely at small businesses

40% say a single six figure attack could end the business for good

88% of SMB breaches involved ransomware, versus 39% at large firms

PREVENTION VERSUS RECOVERY, SIDE BY SIDE

Investment	Cost to prevent	Cost to recover	What you actually get
Security awareness training	A few dollars per user, monthly	Tens of thousands per incident	Stops the click before it happens
Managed detection and response	A predictable monthly fee	$4.44M average breach	Catches intruders in minutes, not months
Backup and disaster recovery	A fraction of one server	Days of downtime, lost data	You restore and keep moving
Doing nothing	$0 today	The whole business, potentially	Hope is not a strategy

A breach is rarely a kicked in door. It is a slow, quiet walk inside.

Hollywood made hacking look like furious typing and a sudden ACCESS GRANTED. Reality is patient and far more ordinary. Most attacks follow the same five stages, and every stage is a chance to stop them, if you are watching.

1. **The lure**
   A convincing email, text, or fake login page lands in an inbox. It looks routine, an invoice, a password reset, a note from the boss.
2. **The click**
   Someone clicks. Credentials are handed over, or a hidden payload quietly installs. The attacker is now inside, often without a single alarm.
3. **The wait**
   This is the dangerous part. Intruders sit quietly, sometimes for weeks, mapping your network and finding the data worth stealing.
4. **The move**
   They escalate access, reach the crown jewels, and disable your backups so you cannot simply restore your way out.
5. **The hit**
   Data is stolen, systems are locked, and a ransom demand appears. By now the damage is done and the clock is loud.

Why this matters

Notice how many steps happen **before** the ransom note. Every one of them is a layer where a strong framework can catch the intruder. One wall might fail. Five rarely do. **That is the entire case for defense in depth,** which is exactly where Chapter 2 goes next.

The number that hurts

The average intruder goes undetected for a long stretch before acting. The faster you see them, the smaller the damage. Detection speed is not a luxury, it is the whole game.

CHAPTER 02

SECURE · THE RISE SERIES

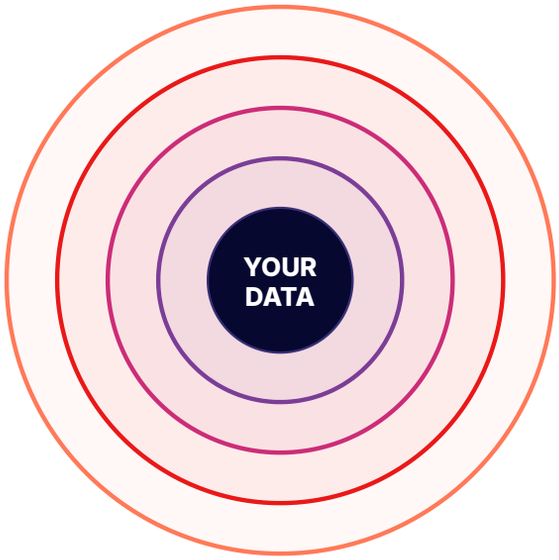
02

Harden Every Layer.

Real security is not one wall. It is many, each one buying you time and catching what the last one missed. Endpoints, detection, response, recovery, defense built in depth.

No single tool saves you. Layers do.

Picture your business as a fortress with rings of protection around what matters most. An attacker has to beat every ring. You only have to make any one of them hold.



- **Testing & hardening**
  Find weak points before attackers do
- **People & awareness**
  A trained team that does not take the bait
- **Network & identity**
  MFA, least privilege, segmented access
- **Endpoints EDR / MDR**
  Devices watched and defended 24/7
- **Data & backups**
  The crown jewels, encrypted and recoverable

ENDPOINT PROTECTION HAS COME A LONG WAY

Capability	Legacy antivirus	EDR	MDR (managed)
Blocks known viruses	✓	✓	✓
Detects new, unknown threats	×	✓	✓
Sees behavior across all devices	×	✓	✓
Human experts hunting 24/7	×	×	✓
Responds and contains for you	×	Some	✓
Shrinks attacker dwell time	×	Some	✓

When prevention fails, recovery is everything.

Even the best defended business should plan to be hit. The difference between a bad week and a closed business is simple, can you restore clean data fast? That is the entire job of backup and disaster recovery, and the rule that governs it has not changed in decades because it works.

THE 3, 2, 1 RULE, SIMPLE AND UNBREAKABLE

3 **COPIES**
of your data

2 **DIFFERENT**
media types

1 **COPY**
stored off site

97%

of organizations with solid backups recovered their encrypted data, and 53% were back within a week

Sophos / industry reporting, 2025

$1.9M

average saved per breach by teams using AI and automation in defense

IBM 2025

The catch nobody talks about

Having a backup is not the same as having a backup that **works**. Backups fail silently all the time, a full disk, a misconfiguration, a job that quietly stopped running months ago. The only backup you can trust is one you have **tested by actually restoring it.** The next page is a true story about exactly why that matters.

How a backup at someone's house saved a $100 million movie.

Late 1998
Deep into production on Toy Story 2, the entire film lives on a shared studio server. Two years of work by hundreds of artists.

A single command
Someone runs a delete command on the wrong directory. On screen, the movie begins erasing itself. First Woody's hat, then his boots, then Woody himself, gone in seconds.

They pull the plug
Engineers yank the machine offline, but roughly 90% of the film is already deleted. Panic sets in.

Backups, the gut punch
They turn to the backups, only to discover they had been quietly failing for about a month. The safety net was not there.

The accidental hero
A technical director had recently had a baby and was working from home, so she kept a full copy of the film synced to a computer at her house, an off site backup, by happy accident.

Wrapped like a newborn
The team drives to her home, carefully wraps the computer in blankets, and transports it back to the studio like a fragile passenger. The film is saved.

~90%
of the film deleted by one command

~2 yrs
of work hanging in the balance

1 copy
off site, the only thing that saved it

The lesson for your business

Pixar did not survive on luck alone. They survived because, by accident, the **3, 2, 1 rule** was in play, an extra copy, on different hardware, stored off site. The real failure was the backup that ran for a month without anyone noticing it had stopped. **Do not be the company that finds out its backups are broken on the worst day of its life.** Test your restores, keep a copy off site, and never bet the business on a safety net you have not pulled on yourself.

CHAPTER 03

SECURE · THE RISE SERIES

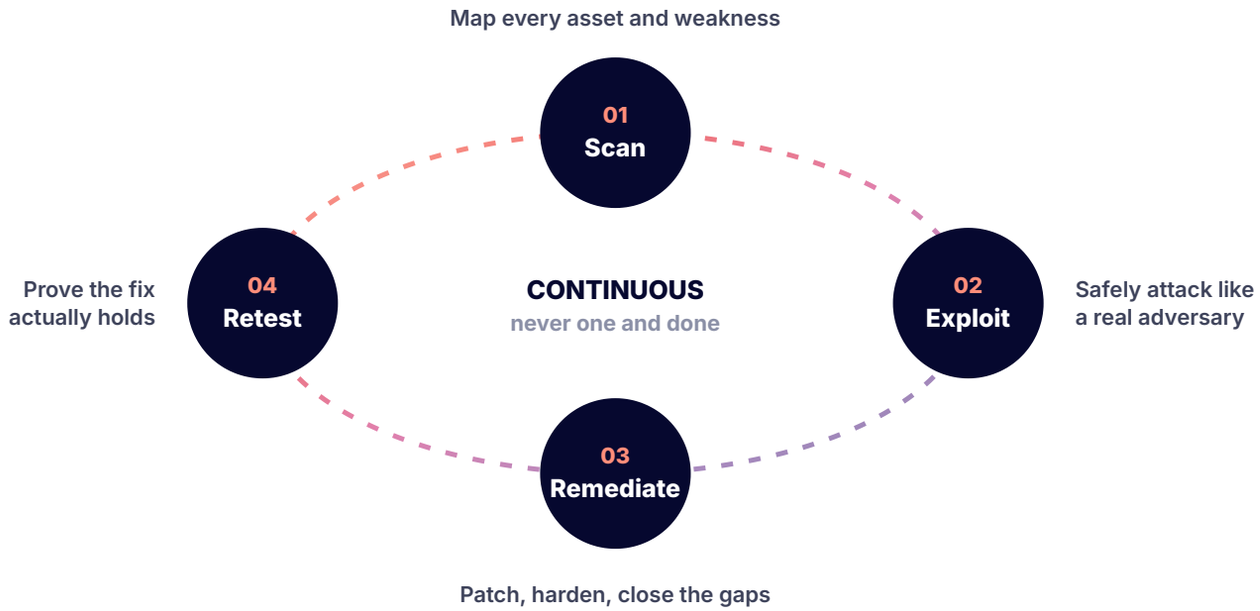
03

Test It Before They Do.

You do not know a wall holds until someone tries to break it. So we try first. Pen testing and breach simulation turn unknown weaknesses into a fixed checklist, on your terms.

Hardening is a habit, not a one time event.

Threats change weekly, so testing cannot be a once a year box to tick. The strongest networks run a continuous loop, probing themselves the way a real attacker would, then closing every gap they find.



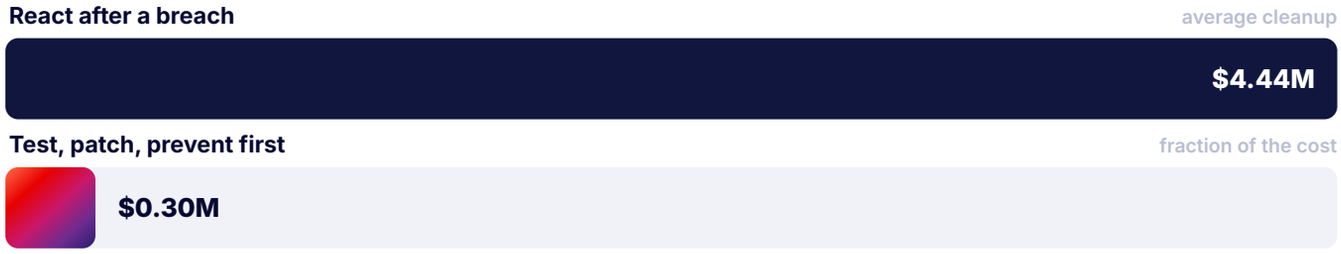
THREE WAYS TO TEST, AND WHEN TO USE EACH

	Vulnerability scan	Penetration test	Breach simulation
What it does	Lists known weak spots automatically	Ethical hackers try a real break in	Runs constant, safe mock attacks
How often	Continuously	A few times a year	Always on, every day
Finds the unknown	✗	✓	✓
Tests your response	✗	Some	✓
Best for	Baseline hygiene	Deep, point in time proof	Ongoing assurance

Finding the crack yourself is far cheaper than letting them.

Most damaging breaches walk in through a door that was already known to be weak. Proactive testing flips the economics entirely. You spend a little to find issues on a Tuesday, instead of spending everything to survive a Friday night incident.

Cost of reacting vs cost of preventing



THE SECURITY MATURITY LADDER, WHERE DO YOU STAND?

Level 1	Level 2	Level 3	Level 4
Exposed	**Reactive**	**Proactive**	**Resilient**
Basic antivirus, no monitoring, untested backups. Hope is the plan.	Tools in place, but you only act after something breaks. Always a step behind.	Layered defense, 24/7 monitoring, regular testing. You catch threats early.	Continuous testing, trained people, tested recovery. You bend, you do not break.

Most businesses sit at Level 2, and do not know it

They have bought the tools, so they feel covered. But owning a smoke detector is not the same as testing it. The goal of a secure framework is to move you up the ladder to **resilient,** where an incident is a manageable event, not an existential one.

CHAPTER 04
SECURE · THE RISE SERIES

04

Your People Are The Perimeter.

The most advanced firewall in the world still cannot stop someone from clicking a convincing email. Your team is either your weakest link or your strongest defense. Training decides which.

Most breaches do not break in. They get invited in.

Attackers learned long ago that it is easier to fool a person than to defeat a system. The good news, the very same people are also your fastest, cheapest layer of defense, once they know what to look for.



of all breaches involve a human action, a click, a reply, a mistake

Verizon DBIR 2025

<60s median time to fall for a phishing email once it lands

16% of breaches begin with phishing as the very first move

90%+ of account attacks blocked by multi factor authentication

SOCIAL ENGINEERING, DECODED

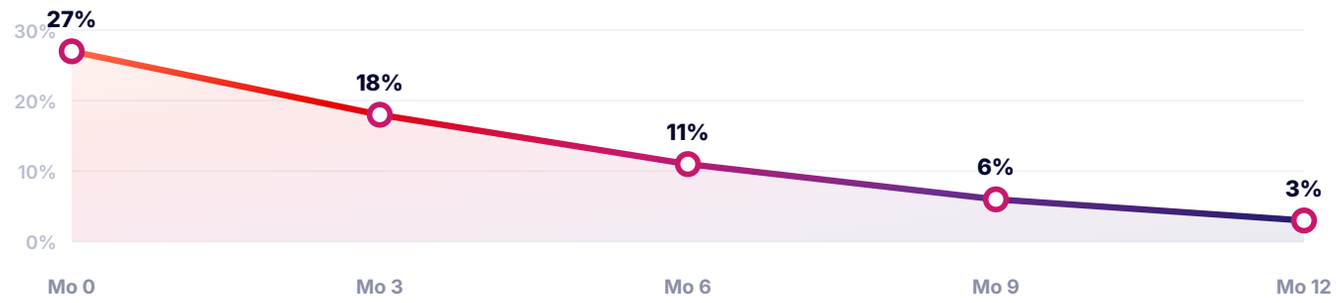
Tactic	How it works	The tell
Phishing	A fake email or text urges you to click or log in	Urgency, odd sender, links that do not match
Spear phishing	A targeted message using your real details	Too personal, asks you to break normal process
Business email compromise	A spoofed boss or vendor requests a payment	New bank details, pressure to keep it quiet
Pretexting	A believable story to extract info or access	A stranger who needs something fast

A trained team is the highest return security you can buy.

Awareness training is not a yearly video nobody watches. Done well, it is a steady drumbeat that rewires habits. The payoff shows up fast, and it compounds.

Phishing click rate falls as training takes hold

ILLUSTRATIVE



Teach the basics

Short, regular lessons on spotting fakes, building passwords, and reporting anything odd.

Test with real lures

Safe, simulated phishing that shows who clicks, with coaching instead of blame.

Track and improve

Click rates fall month over month as habits stick and awareness becomes second nature.

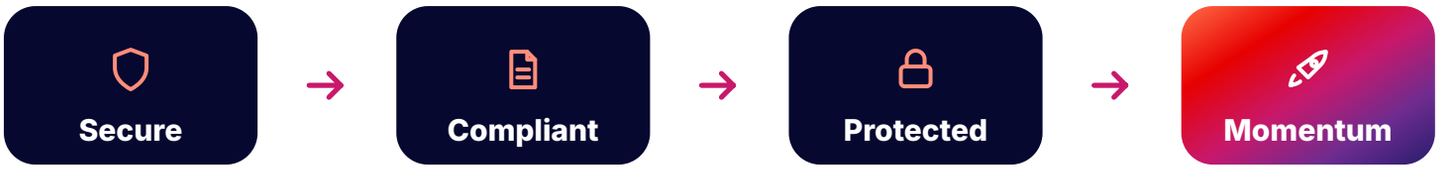
Make it culture

Reporting a suspicious email becomes a win, not an embarrassment. Everyone owns security.

THE PAYOFF

Secure is not the goal. It is what frees you to move.

A secure foundation makes compliance almost automatic, compliance protects your business and your data, and a protected business is free to do the one thing that matters most, keep building momentum.



YOUR SECURE FRAMEWORK, ON ONE CHECKLIST

- **Layered endpoint protection**
  EDR or MDR on every device, watched around the clock
- **Multi factor everywhere**
  The single cheapest block against stolen passwords
- **Tested 3, 2, 1 backups**
  Restores proven, not assumed, with a copy off site
- **24/7 monitoring and response**
  Someone watching when you are asleep
- **Regular testing**
  Scans, pen tests, and simulations on a schedule
- **Security awareness training**
  Your people turned into a human firewall
- **Least privilege access**
  People reach only what they actually need
- **A written incident plan**
  Everyone knows their role before the bad day

ONE FOUNDATION, MANY FRAMEWORKS

CMMC · HIPAA · NIST · SOC 2 · PCI DSS · GDPR

SOLUTION BUILDERS®

RISE · S is for Secure

Your secure foundation starts with one conversation.

Solution Builders designs cybersecurity from the ground up, endpoints, detection, recovery, testing, and the human firewall, all working as one framework. Let us show you where you stand on the maturity ladder, and exactly how to make your momentum unbreakable.

TALK TO A SECURITY ARCHITECT
www.solutionbuilders.com

BOOK A FREE DISCOVERY SESSION
No pressure, just a plan

RESILIENT · INTEGRATED · SECURE · EVOLVING

Figures cited from IBM Cost of a Data Breach 2025, Verizon Data Breach Investigations Report 2025, and published SMB security research. The Toy Story 2 account is drawn from “Creativity, Inc.” by Ed Catmull. Charts marked illustrative are for explanation, not forecasts.