



AI and Cyber Security Foundations

Practical knowledge for all businesses

PRESENTED BY SEAN HIEBERT · STILLWATER **IT** SOLUTIONS
SESSION DATE: AUG 6, 2026



Sean Hiebert
FOUNDER, STILLWATER IT

WELCOME

I'm **Sean Hiebert**, founder of StillWater **IT** Solutions. We're the managed IT partner for professional services and trades across the BC.

Today is not a sales pitch. It's designed to make your daily work safer and smarter.

This session is yours. Ask anything. Nothing is too basic.

What we'll cover

01

CYBER SECURITY FOUNDATIONS · 25 MIN

How attacks really happen, and the four daily habits that block almost all of them.

02

AI FOUNDATIONS · 20 MIN

What AI is, what it is not, and where your data goes when you use it.

03

YOUR PLAYBOOK · 15 MIN

The five things you'll do differently on Monday.

Stop me at any time with questions.

Most teams never get formal training on this



Training lags technology

AI tools and attack methods change every few months. Most staff training happens once, at onboarding, if at all.



Everyone is a target

Attackers don't just aim at IT. They aim at whoever answers the phone or opens the inbox first.



Confidence outpaces caution

Teams that feel comfortable with AI tools are often the least aware of what they're exposing.

This is exactly the gap StillWater Academy was built to close.

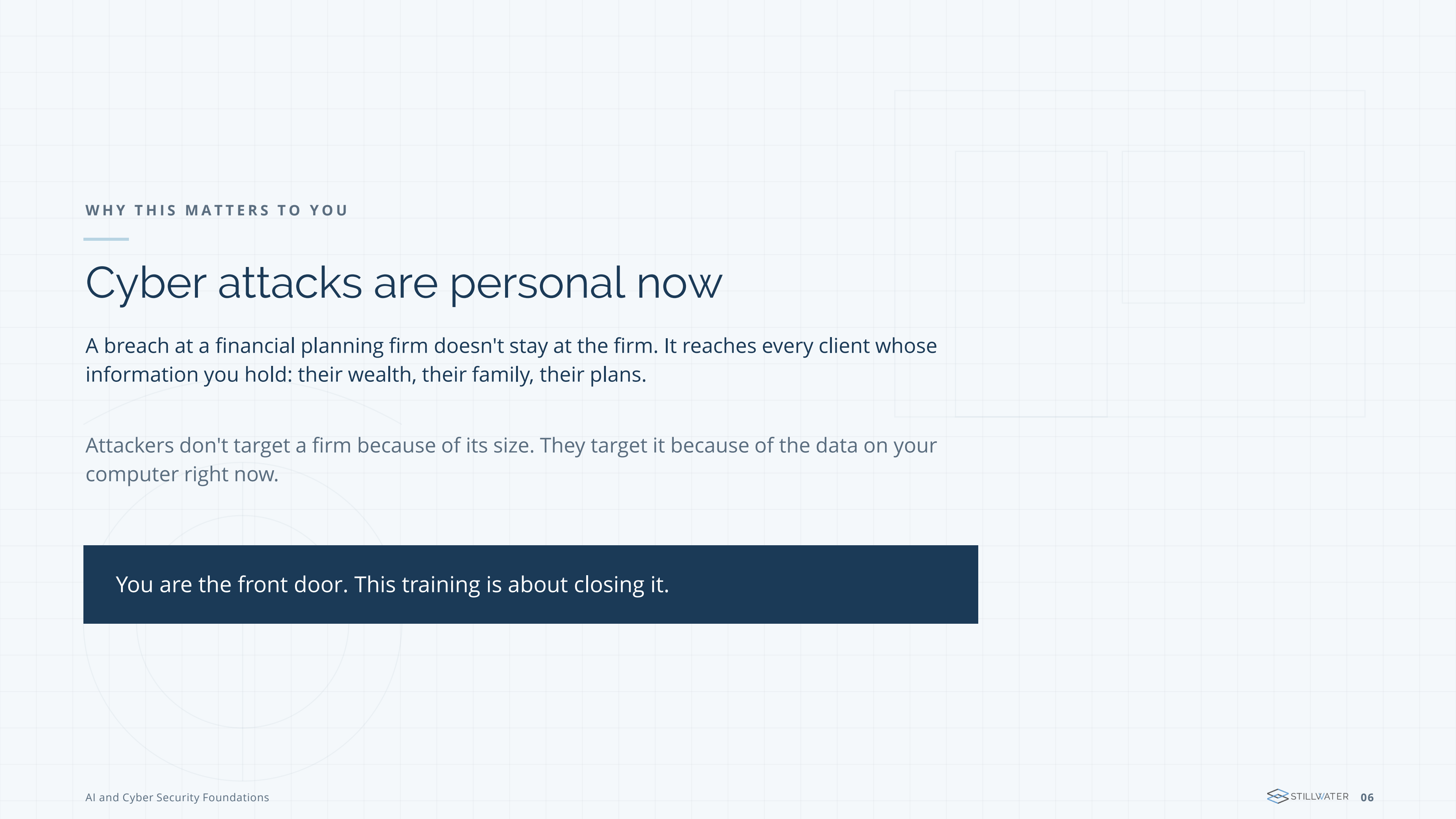
The background is a dark blue field filled with a complex network of thin, light blue lines connecting small white dots. The dots are scattered across the frame, and the lines form a web-like structure that suggests a digital or interconnected environment.

PART ONE

Cyber Security Foundations

How attacks really happen, and how you stop them.

WHY THIS MATTERS TO YOU



Cyber attacks are personal now

A breach at a financial planning firm doesn't stay at the firm. It reaches every client whose information you hold: their wealth, their family, their plans.

Attackers don't target a firm because of its size. They target it because of the data on your computer right now.

You are the front door. This training is about closing it.

The three ways attackers get in

01

Phishing emails

Over 90% of breaches start with a single click.



02

Weak passwords

One compromised login opens every account it touches.



03

Unpatched devices

Outdated software is an open door.

All three are preventable. Daily habits do the work.

Real examples you'll receive this month



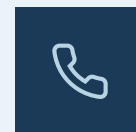
"URGENT: wire instructions changed on the Henderson account. Please update before 3 PM today."

Why it works: urgency, authority, and a real client name pulled from social media.



"Your Microsoft 365 password expires in 24 hours. Click here to keep your account active."

Why it works: it looks like every legitimate IT email you've ever received.



"Voicemail from an unknown caller. Listen attached."

Why it works: curiosity, plus a one-click action.

Rule of thumb: urgency is the tell. Pick up the phone.

Two habits that block almost every account attack



A password manager

Think of it as a fireproof safe. You only remember one key. Inside, every account has a different complex password you never have to memorize.



Two-step login

Even if someone steals your password, they still can't get in without your phone. Use the app-based version, not text messages.

Together, these two stop more than 99% of credential attacks.

Four daily habits



Lock your screen

Every time you step away. Even for a coffee.



Avoid public Wi-Fi

Without a company-approved VPN.



Install updates

The day they arrive. Not next week.



Keep work on work devices

Personal stays personal.

These four habits are boring on purpose. Boring is what works.

Your gut is usually right

1

Pause

Don't click. Don't reply. Don't forward to a colleague to ask.

2

Verify

Pick up the phone. Use a number you already have, never one from the suspicious message.

3

Report

Send it to your designated contact. No penalty for asking. Real penalty for staying silent.

There is no such thing as a stupid security question.

PART TWO

AI Foundations

What it is, what it is not, and where your data goes.

WHAT AI ACTUALLY IS

It's autocomplete, supercharged

Think of the predictive text above your phone keyboard, the little word it suggests next. AI is that same idea, scaled up enormously. It predicts the most likely next words from patterns it learned across billions of documents.

It doesn't know anything. It doesn't understand your client. It predicts what a good answer sounds like.

You type:

"Thanks for your patience, I'll follow up"

up

shortly

soon

AI picks the most likely next word, millions of times over. That's the whole trick.

What it's good at, and what it isn't

GOOD AT

- Drafting a first version of an email
- Summarizing long notes
- Brainstorming options
- Rewording for tone
- Explaining a concept simply

NOT GOOD AT

- Precise math
- Current law or regulation
- Real-time facts
- Anything confidential

Every AI output needs a human editor before it leaves the firm.

When you paste, where does it go?

You paste client info

A statement, a name, a number.



Into a free AI tool

No business agreement in place.



It can't be recalled

It may train the model. You don't get it back.

A simple analogy: a free tool is like discussing a client out loud in a crowded coffee shop. A business account is the private meeting room.

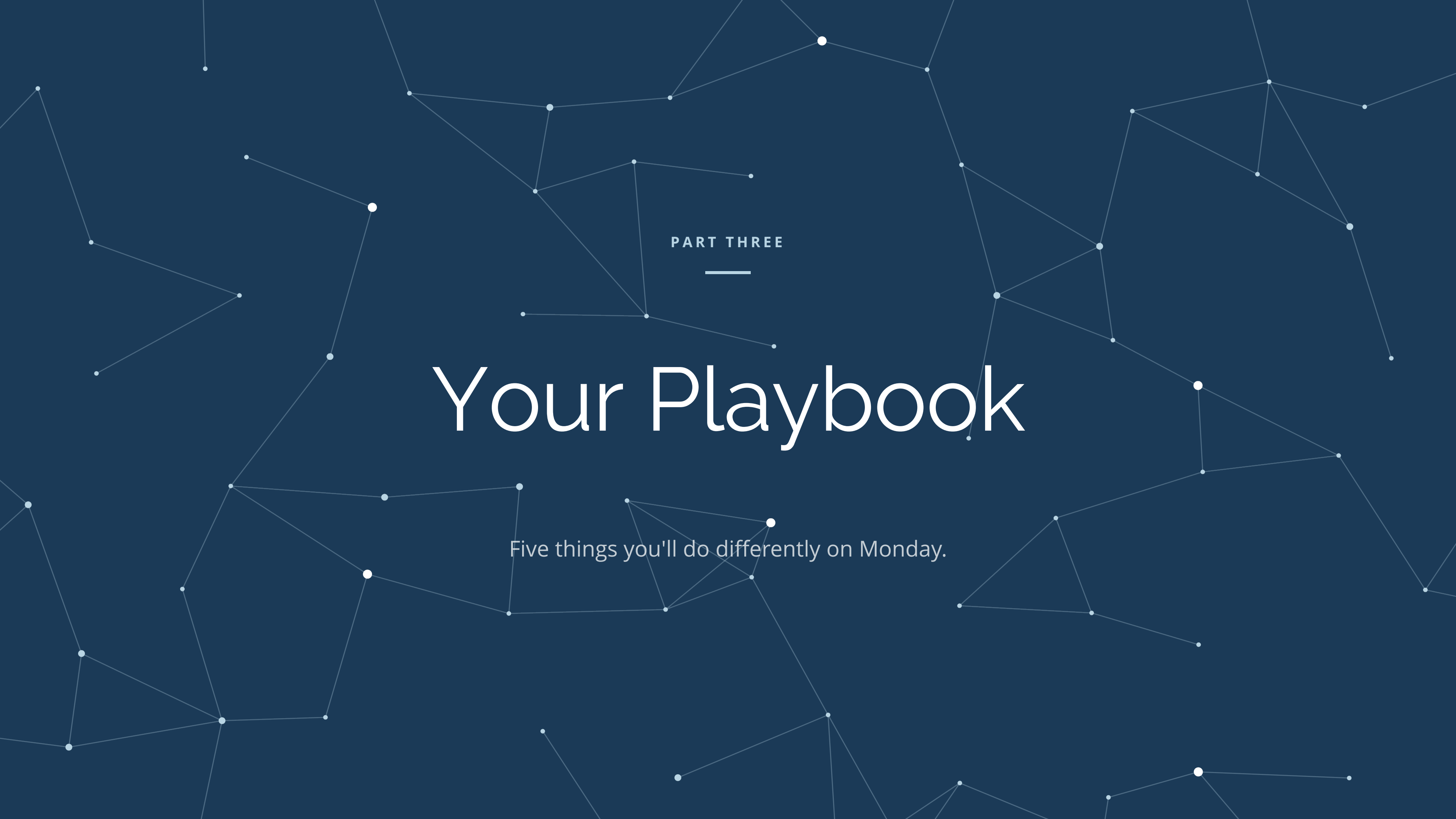
The fix isn't banning AI. It's approved, business-grade accounts with clear rules.

Five rules for using AI at work

- 01 No client names or numbers in any AI tool. Ever.
- 02 Use only approved, business-grade accounts.
- 03 AI drafts. You edit. Every time.
- 04 Verify any number, law, or citation against a primary source.
- 05 Unsure whether a tool is safe? Ask first.

SEAN'S TIP

Treat AI like a confident intern: helpful, eager, occasionally wrong, and never trusted with the keys.



PART THREE

Your Playbook

Five things you'll do differently on Monday.

Five things you'll do on Monday

1 Turn on two-step login for your email and Microsoft 365.

2 Start using the password manager we set up for you.

3 Pause and phone to verify any money or login request.

4 Lock your screen every time you stand up.

5 Keep client information out of every AI tool.

When something feels wrong: Pause. Verify. Report.

604 899 1105 · info@stillwaterit.ca

StillWater Academy builds the foundational skills real businesses need

An interactive online certification portal, self-paced and practical. AI Readiness is the first course; new certifications are added all the time, each focused on skills your team can put to work right away.



Foundational, not theoretical

Practical skills real businesses use every day, taught in plain language.



A growing course library

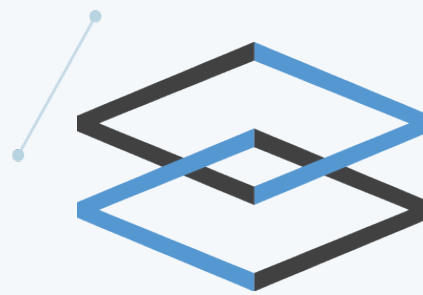
Starts with AI Readiness. New certifications keep arriving as needs evolve.



Certification that verifies

Each course ends in a certificate anyone can verify online.

Now open through a founding membership: get in early and grow with the library as it expands.



Give your team a foundation that keeps growing.

Join the founding membership and get your team certified in the skills real businesses run on, starting with AI Readiness and every course that follows.

thestillwateracademy.com →

604 899 1105 · support@thestillwateracademy.com