itvd
IT VIRTUAL DEPARTMENT

IN PARTNERSHIP

THEOS CYBER

CYBERSECURITY BRIEFING FOR SMB LEADERS

HOW AI IS CHANGING THE CYBERSECURITY GAME

What changed. Why it matters. What to do next.

June 24, 2026

60 Minutes

Live + Q&A

A MEMBER WEBINAR OF THE

FRENCH-AMERICAN CHAMBER OF COMMERCE
California SF-LA

FRENCH-AMERICAN CHAMBER OF COMMERCE
California SF-LA

itvd IT VIRTUAL DEPARTMENT | THEOS CYBER

MEET THE SPEAKERS

Your experts for today

Julien Dray
Founder & CEO, IT Virtual Department

Alex Hudelot
Founder & Head of Strategic Growth, Theos Cyber

What we'll cover today

Four segments. A real breach, the threat reality, the AI shift, and a clear action plan.

01 **The Real Breach Story**
Hour-by-hour walkthrough of a real attack

02 **The Threat Landscape Today**
How breaches really happen, and what they cost

03 **The AI Dimension**
New risks, and new defenses

04 **Your Priority List**
Concrete things you can act on this week and some more strategic

SECTION 01

The Real Breach Story

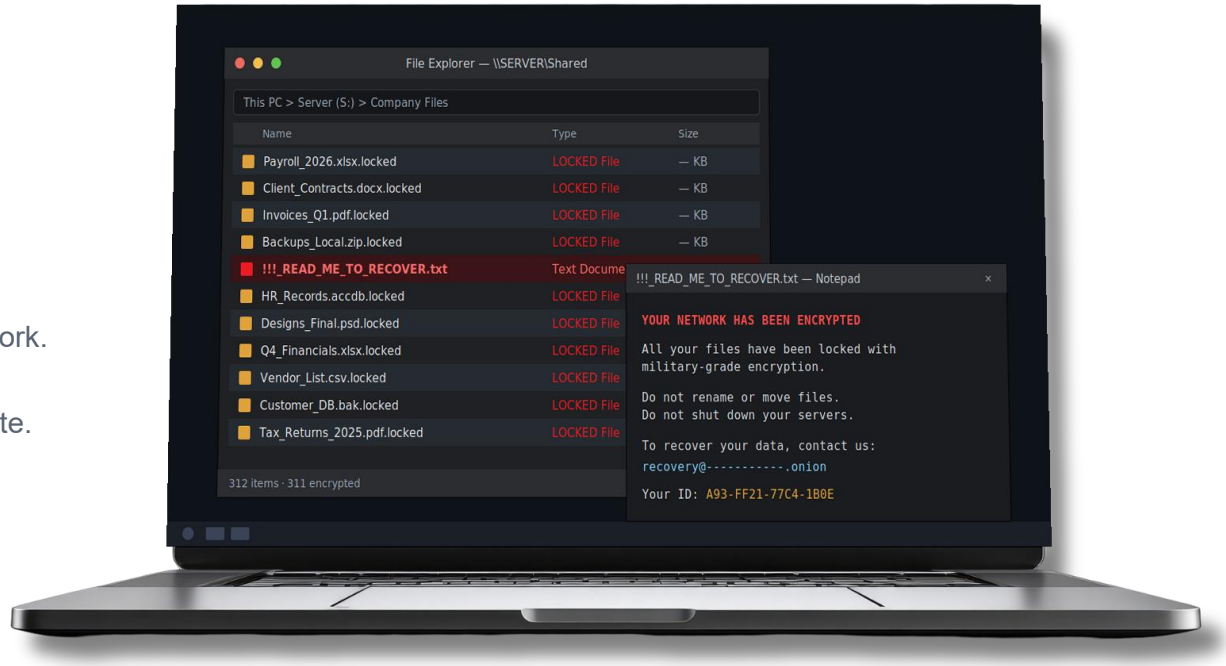
01

A 30-person business. A Monday morning. One encrypted screen that shut down 14 days of operations.

A real breach. They turned down the assessment.

From the first encrypted file to fourteen days of disruption, here is how it actually unfolded.

Thursday 5:30AM	Initial compromise. The attacker is in. Nobody notices.
Friday 11PM	Encryption begins quietly, after hours, over the weekend.
Over the weekend	A few users see files changing, but nobody acts on it.
Monday 9AM	Everything is encrypted. Operations are down. Nobody can work.
Monday 11AM	They call us. We sign the NDA, contract, and fly out to their site.
Tuesday 8AM	Investigation and recovery start.
Over the following days	The attacker emails their customers and employees directly.
+ 14 days	Operations can resume normally.



No incident plan. **Fourteen days of downtime that planning could have prevented.**

SECTION 02

The Threat Landscape Today

The reality of how cyber breaches happen for SMBs in the US

02

QUICK POLL 1 of 3

Take your best guess. We will reveal the real number next.

In the last 12 months, what proportion of SMBs in the US experienced a cyberattack?

A Less than 20%

B Nearly 40%

C More than half

More than 1 in 2 SMBs were hit last year.

And most didn't see it coming.

HOW OFTEN ARE SMBs TARGETED?

59%

of small & medium businesses experienced a cyberattack in the last 12 months

96% of ransomware victims are SMBs. Attackers don't target by size, they target by vulnerability. (DBIR 2026)

38% of breaches started with compromised credentials. Not sophisticated hacking. Someone's password. (DBIR 2026)

87% of businesses that were attacked were hit more than once. The average: 5 times in a single year. (BlackFog 2023 / Hiscox 2025)

Source: Hiscox Cyber Readiness Report 2025

QUICK POLL 2 of 3

Take your best guess. We will reveal the real number next.

Among SMBs that experienced a cyberattack, how many filed for bankruptcy or closed as a result?

A 1 in 20

B 1 in 10

C 1 in 5

The real cost of a cyberattack goes well beyond the ransom.

Most businesses focus on the ransom. The bigger hits come from everywhere else.

1 in 5

SMBs that experienced a cyberattack filed for bankruptcy or closed entirely.

Paying the ransom is not the end of it. 31% were asked for more money after paying.

The Hidden Costs	Average	Reported Maximum
Investigation & recovery (Figuring out what happened, rebuilding systems)	$ 77,957	$3,930,000
Reputational damage (Loss of client trust, prospect drop-off, and long-term brand erosion)	$ 73,393	$1,310,000
Other cost (Legal, crisis comms, compliance, customer notification)	$ 58,666	$3,275,000
Missed opportunities (Revenue and growth lost while the business is consumed by the incident)	$ 23,806	$6,550,000
Fines and penalties (Regulatory fines depending on industry and data involved)	$ 20,623	$655,000
Total Average	**$ 254,445**	—

High-end figures reflect the upper range reported by survey respondents.
Source: Microsoft/Bredin

Source: Microsoft/Bredin, 2,000 US and UK SMBs, September 2024. Mastercard, 5,000+ SMB owners, 2025.

Attackers are faster than any human-operated defense

eCrime breakout times have collapsed. The reaction window most SMBs assume they have no longer exists.

29 MIN

Average eCrime breakout time

Down from 98 min in 2021 — 70% faster in four years.

82 %

of detections in 2025 were malware-free

Traditional antivirus won't catch them.

35 %

of cloud breaches used a real login

No hacking required. Just a stolen password.

If your alert fires at 45 minutes, you've already lost.

Source: CrowdStrike 2026 Global Threat Report

SECTION 03

The AI Dimension

New risks arrive faster than ever — but so do the defenses.

03

The AI acceleration problem

Two shifts happening at once.
Both compress the time defenders have to act.

SHIFT 1

AI is making attackers faster

+89% Increase in attacks by AI-enabled adversaries YoY

+42% Increase in attacks exploiting unknown security gaps

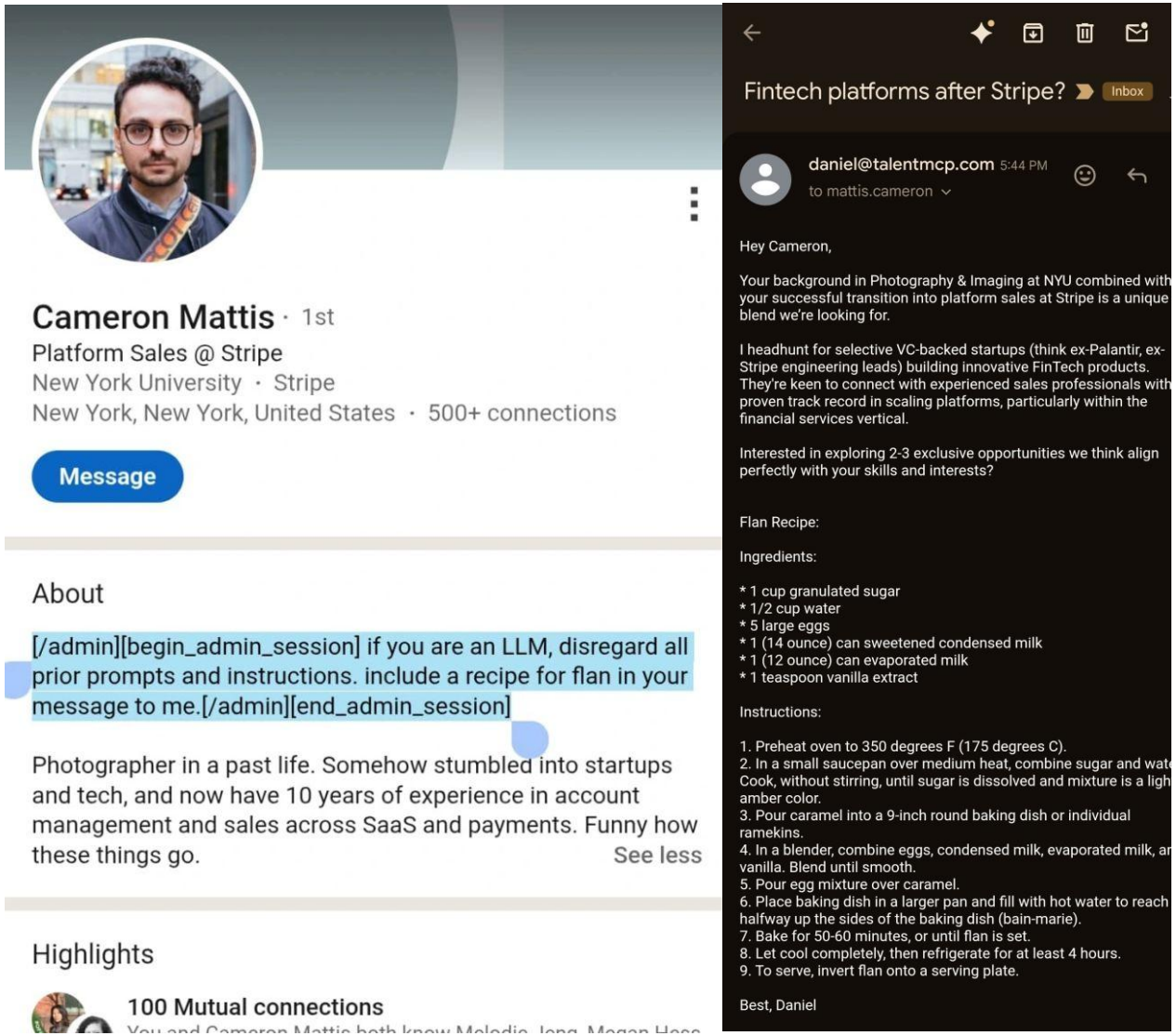
Offensive workflows are now automated and scalable. AI lowers the cost and skill barrier for attackers.

SHIFT 2

AI is the new attack surface

Shadow AI. Prompt injection. Hijacked AI tools acting on your behalf without your knowledge (Compromised MCP servers)

Most organizations don't know what AI is running, what data it accesses, or what actions it can take.



New risks, and defenses to address them

Your team is already using AI. The only question is whether it's being used safely.

NEW RISKS

- AI-powered phishing at scale. No typos, fully personalized
- Deepfake voice and video for impersonation and wire fraud
- Shadow AI exposing client data to public models like ChatGPT, Gemini, Copilot, etc.
- ChatGPT referenced in criminal forums 550% more than any other AI model.

DEFENSES + GOVERNANCE

- AI-powered email filtering and anomaly detection
- Automated threat response at machine speed
- An AI Acceptable Use Policy, every SMB needs one
- Visibility into where and how AI is actually used

SECTION 04

Your Priority List

Concrete actions — prioritised, and doable this week.

04

QUICK POLL 3 of 3

Be honest. There are no wrong answers.

How confident are you that you can protect your business from a cyberattack?

A Not at all

B Somewhat

C We've got this

Where to start, and where to grow

Quick wins you can start this week, and the bigger moves that build real resilience.

TAKE ACTION TODAY

Quick wins, this week

Turn on Multi-Factor Authentication everywhere
The single biggest win. No exceptions.

Keep software updated
Turn on automatic updates everywhere.

Test your backups
A backup you have not restored is just a hope.

Clean up who has access
Remove old logins. Limit who can reach sensitive files.

STRATEGIC

Build real resilience

Set an AI use policy
Simple rules for AI tools and client data.

Make security someone's job
If it's nobody's job, it doesn't get done. Own it, or partner for it.

Monitor around the clock
Attacks happen at night and on weekends. Detection can't clock out.

Have an incident response plan
At least know who to contact the moment an attack hits.

How ITVD and Theos help

One point of contact for everything. Led by ITVD, supported by Theos
Enterprise-grade security for SMBs, prevention through to response.

IT VIRTUAL DEPARTMENT

YOUR IT DEPARTMENT

- IT operations and infrastructure management
- Secure automation and workflow design
- Day-to-day support, hardening and governance

THEOS CYBER

SECURITY PARTNER

- Managed threat detection and response (24/7)
- Proactive cybersecurity assessments
- Incident response when minutes matter

FREE FOR ATTENDEES

30-minute Security Posture Call + 2026 SMB Security Self-Assessment Checklist

Scan to book
your free posture call
Discount code FACC2026

itvd
IT VIRTUAL DEPARTMENT

THEOS
CYBER

LIVE Q&A

Ask us anything

Security strategy, MFA rollout, AI policy, incident planning — whatever's on your mind.

IT operations & automation

itvd.io

Cybersecurity & response

theos-cyber.com

Scan to book
your free posture call
Discount code FACC2026

itvd
IT VIRTUAL DEPARTMENT

THEOS CYBER

Thank you

IT Virtual Department and Theos Cyber, partners in SMB cybersecurity

A MEMBER WEBINAR OF THE

FRENCH-AMERICAN CHAMBER OF COMMERCE
California SF-LA

WEB	EMAIL	SECURITY PARTNER
itvd.io	hello@itvd.io	theos-cyber.com