AN EXECUTIVE BRIEFING FOR BUSINESS OWNERS

The Quiet War on Your Business.

Cyber Fraud & Security in the Age of AI-Powered Crime

Brandon Lockett, Chief Executive Officer
Neutron Engineering · Managed IT & Cybersecurity, built for businesses that run on trust

Small Business Summit · Nashville, TN · May 2026

Who we are, and why I'm up here.

The 40 minutes ahead — and the promise I'll make you.

NEUTRON ENGINEERING

Managed IT and cybersecurity for businesses that can't afford a Tuesday-morning surprise.

- 24×7 US-based Security Operations Center
- Built around regulated, finance-adjacent businesses
- A single accountable partner — not a vendor zoo
- Plain-English reporting for owners and boards
- Team leaders with banking, audit, and examiner backgrounds

THE PROMISE

You will leave this room with five things you can act on Monday.

- A clearer picture of what's aimed at businesses your size
- The fraud playbook — with this year's real numbers
- The rules regulators now quietly expect, not just recommend
- Five no-cost actions to reduce risk this quarter

A NUMBER WORTH HOLDING IN YOUR HEAD

$16.6B

in reported cybercrime losses in a single year — up 33% on the year before.

859K

complaints to the FBI — roughly one every 37 seconds

$2.77B

lost to Business Email Compromise alone

1 in 6

breaches now involve AI on the attacker's side

Sources: FBI IC3 2024 Annual Report · IBM Cost of a Data Breach 2025

Here's where we're going.

40 minutes. No vendor theatre. Just what we see every week.

01 **The new threat landscape**

Who's hunting small businesses right now — and why the game just changed.

02 **The attacker's playbook**

BEC, wire fraud, ransomware, vendor compromise, check fraud.

03 **AI-enabled fraud**

Deepfakes, voice clones, and industrial-scale phishing.

04 **The regulatory bar**

FTC, state privacy, PCI, cyber-insurance fine print.

05 **What "good" looks like**

A simple framework — and the gaps we see most often.

06 **Where we fit**

Five actions you can take Monday, with or without us.

SECTION 01 · THE THREAT LANDSCAPE

The attacker on the other side of your firewall has changed.

You are no longer being targeted by a hoodie in a basement. You're being worked by professional organizations with HR, QA, and quarterly targets.

Organized Crime Syndicates

Run like startups. They recruit, pay bounties, and specialize by function.

Nation-State Spillover

Tools built for geopolitical operations leak, get resold, and end up in criminal kits.

AI-Augmented Fraudsters

Generative AI has collapsed the cost of a convincing phishing email, voice, or video.

Access Brokers & Insiders

Legitimate credentials are now a commodity — bought, not stolen, and sold by the batch.

And small businesses are the sweet spot.

Real money. Lean teams. Same-day regret. Attackers know the math.

Profile	LARGE ENTERPRISE	SMALL BUSINESS
Security as % of IT budget	~15%	**Under 5%**
Dedicated security staff	100+	**0 — 1**
24×7 monitoring	In-house	**Rarely**
Value of data held	High	**Identical**
Runway if operations stop	Cushioned	**Existential**

Regulators judge you on the same yardstick as a Fortune 500. Attackers pick you because you aren't one.

Six ways money leaves your business this year.

Business Email Compromise

Spoofed vendors, rushed wires — the quiet $2.77B drain.

Wire & ACH Fraud

Same-day rails, instant payments, same-day losses.

Ransomware

Encrypt, exfiltrate, extort — often all three at once.

Vendor Compromise

Your payroll service. Your CPA. Your law firm. Their breach, your loss.

AI Voice & Deepfake

A 20-second call is enough to clone your CFO's voice.

Check Fraud Resurgence

Mail theft and check-washing are back with a vengeance.

Business Email Compromise: the $2.77B con that keeps working.

No malware. No exploit. Just a convincing email at exactly the wrong moment.

BEC BY THE NUMBERS

$2.77B

reported U.S. losses in 2024

$8.5B

BEC losses 2022–2024 combined

63%

of organizations hit by BEC last year (AFP 2025)

The attack chain, start to finish

1. **Recon**

   Scrape LinkedIn, org charts, prior vendor emails — all freely available.

2. **Footprint**

   Compromise a mailbox (often upstream, at a vendor you trust) or spoof a look-alike domain.

3. **Pretext**

   Wait for a real invoice, real closing, or real payroll run to attach the fraud to.

4. **Strike**

   Urgent wire change, after-hours, with plausible business context. Funds gone in minutes.

Sources: FBI IC3 2024 · AFP 2025 Payments Fraud & Control Survey

Faster rails. Faster losses.

Same-day ACH, RTP, FedNow — the settlement window has collapsed. Controls built for T+1 don't work at T+0.

The window that closed

Funds used to sit overnight. Now they clear in seconds and leave the country before dawn. Recovery odds fall roughly in half every 24 hours.

Friday at 4:00

Classic attack timing. Staff tired, approvers out, pressure to close the week. Almost every BEC wire we've unwound was initiated inside this window.

The call-back myth

Calling the number in the email is no call-back at all. Independent verification — number from your records, challenge phrase — is now table stakes.

The FBI's Recovery Asset Team stops roughly two-thirds of reported BEC wires — but only if you call within hours, not days.

Ransomware: it isn't "if" — it's the Tuesday you find out.

Today's attackers don't just lock you out. They steal first, then lock, then publish if you don't pay.

ENCRYPT

Operations stop. Payroll, billing, client files — all unreadable.

EXFILTRATE

Your client data is copied out before encryption. They already have it.

EXTORT

Pay, or the data is leaked to your clients, your regulators, and the press.

9%

year-over-year rise in ransomware complaints in 2024 (FBI IC3)

24 days

average business downtime after a ransomware incident

~50%

of victims who pay still cannot fully restore their data

Sources: FBI IC3 2024 · Sophos State of Ransomware · industry benchmarks

SECTION 03 · THE AI TURN

The moment the attacker's voice sounded exactly like your CFO.

Three things have become trivial in the last 18 months. Your defenses were designed before any of them were.

Voice cloning

20 seconds of audio from a podcast, earnings call, or voicemail is enough. Cost to the attacker: near zero.

Deepfake video calls

A finance clerk in Hong Kong wired $25M off a single video call with a fake CFO. Not theoretical.

Phishing at scale

Grammatically perfect, personalized to your deal, sent in your CEO's voice — drafted in under a minute.

1 in 6 breaches in 2025 involved AI on the attacker's side · **37%** used AI for phishing · **35%** for deepfake impersonation

Source: IBM Cost of a Data Breach Report 2025

Their breach. Your headline.

You do not control your vendors' controls. But you do answer for the data you handed them.

The vendors that touch your money and your data

- Payroll and HR platform
- Accounting and bookkeeping provider
- Outside counsel & CPA
- Cloud file storage, CRM, e-mail
- Core banking / treasury provider
- Managed IT or help-desk vendor
- Benefits broker & retirement admin

THE UNCOMFORTABLE REALITY

Every one of those vendors is a separate attack surface — and their breach notification clause decides how much trouble you're in.

- Most SMBs cannot name every vendor holding client data
- Fewer than 1 in 5 have reviewed a vendor SOC 2 report in the last year
- Contracts often place the burden of disclosure on you, not them
- Major breaches — MOVEit, Snowflake, Change Healthcare — landed on small businesses, not the headline brands

SECTION 04 · THE REGULATORY BAR

The rules quietly became expectations.

"We're too small for that" is no longer a defense. Much of this already applies to businesses in this room.

FTC Safeguards Rule

Written info-security program, named qualified individual, MFA, encryption, vendor oversight, incident response. Applies to most financial-services SMBs.

SEC Cyber Disclosure

Material cyber incidents disclosed on Form 8-K within 4 business days. The definition of "material" is broader than most owners assume.

State privacy cascade

CCPA, Colorado, Connecticut, Texas, Tennessee, and a dozen others. Notification windows as tight as 30 days — some faster for medical data.

Cyber-insurance fine print

MFA, EDR, backup isolation, tested IR plan. Miss any and the policy may not pay — you'll find out during the claim.

What does one bad Tuesday actually cost?

The invoice keeps arriving long after the incident ends.

AVERAGE BREACH COST, FINANCIAL SERVICES

$5.56M

per incident in 2025. The global average is $4.44M. In the U.S., it's $10.22M.

241 days

average time to identify and contain a breach.

What's actually in that invoice

- **Detection & response**

  Forensics, outside counsel, emergency engineering, containment.

- **Notification & credit**

  Mailed notices, monitoring for affected customers and employees.

- **Business disruption**

  Lost revenue, idle staff, missed deadlines, penalties on contracts.

- **Legal & regulatory**

  Class-action defense, state AG inquiries, regulatory fines.

- **Customer churn & trust**

  The longest-running cost — it shows up in next year's renewals.

Source: IBM / Ponemon Cost of a Data Breach Report 2025

SECTION 05 · WHAT GOOD LOOKS LIKE

Six things every well-run business has in place.

Aligned to NIST Cybersecurity Framework 2.0 — the common language regulators and insurers now speak.

GOVERN

Owner-level accountability. Written program. Risk accepted on purpose, not by accident.

IDENTIFY

Know your data, your vendors, and where money and sensitive information move.

PROTECT

MFA everywhere, EDR on every endpoint, hardened identity, isolated backups.

DETECT

24×7 eyes on the network. Alerts triaged by humans, not by a voicemail.

RESPOND

A written incident-response plan. Tabletop-tested. Legal and PR on speed dial.

RECOVER

Tested restores. Communication plan. Lessons fed back into controls.

Where small businesses most often fall short.

What we find on day one of nearly every assessment.

01

MFA — partial, not universal

Multi-factor is on email, missing on VPN, remote desktop, finance apps, and privileged accounts. Attackers walk in through the gap.

02

EDR — an antivirus product, not a response capability

A tool humming in the corner with nobody watching it at 2 a.m. is a checkbox, not a control.

03

Backups — there, but not tested

We find backups that haven't been restored in over a year — or that are on the same domain the attacker will own first.

04

Email — authenticated but not enforced

SPF and DKIM configured. DMARC in "monitor only." Lookalike domains flying through.

05

Incident response — a document, not a rehearsal

A PDF in a shared drive is not a plan. One 90-minute tabletop exposes nearly every weakness.

06

Vendor oversight — handshake, not paperwork

Critical vendors without reviewed SOC 2 reports or a written breach-notification clause.

A story from last quarter.

Names and numbers have been changed. Everything else is real.

THE SETUP

42-person financial-advisory firm. Friday, 3:47 p.m.

- Controller receives an internal Teams message from "the CEO"
- Follow-up call — the CEO's voice, exact cadence — asks for a $148K wire to close an acquisition before the weekend
- Controller ready to execute. Called the CEO's mobile to confirm — out of habit, not policy
- Real CEO had no idea. Voice cloned from a 90-second conference panel on YouTube

WHAT CHANGED IN THE NEXT 30 DAYS

A call-back policy isn't a policy until you script it.

- Mandatory two-person approval on any wire over $25K
- Verbal challenge phrase rotated monthly, never over email
- Wire-change requests verified against a number from the system of record — not the request itself
- Deepfake-awareness tabletop run with the entire finance team
- **Result: two attempted follow-up attacks caught in the next 60 days**

The math of building this in-house simply does not work below about 500 people. That's the reason managed services exist.

Building it yourself

- A mid-level SOC analyst runs $110K+ fully loaded — and you need at least three for real 24×7
- $300K+/year in tooling (SIEM, EDR, email security, vulnerability mgmt)
- 6–9 months to stand up, longer to tune
- Single point of failure when the key person leaves
- Still need outside help during an incident

Partnering with an MSP firm like Neutron

- 24×7 US-based SOC on day one
- Enterprise tool stack included in a predictable monthly fee
- Onboarded in 90 days, measurable results in 30
- A bench, not a person — no single point of failure
- Incident-response retainer built in, not bolted on

What Neutron actually does.

Four service lines, one accountable partner, one monthly invoice.

Managed IT

Help desk, endpoints, networking, cloud, Microsoft 365 — the plumbing that keeps your people working.

Managed Security

24×7 SOC, EDR/XDR, email defense, identity & access, vulnerability management — the watch on the wall.

Compliance & Audit

FTC Safeguards, state privacy, PCI, SOC 2 readiness — the paperwork regulators want, in plain English.

Advisory

Virtual CISO, tabletop exercises, M&A cyber due diligence, board-level reporting that doesn't insult the reader.

The numbers we manage to.

Representative outcomes across our client base — the metrics we report on every month.

< 15 min

Median time to detect a serious incident across the SOC

92%

of security alerts triaged without reaching the client

40%+

Reduction in help-desk volume within 90 days of onboarding

0

Audit findings unresolved at year-end across managed clients

Client-specific numbers vary by scope and starting baseline. Benchmarks available under NDA on request.

Five things to do Monday — whether you hire an MSP or not.

No budget required. Every one of these blocks a real attack we've seen this year.

1. **Turn on phishing-resistant MFA on every account that touches money or email**
   Authenticator app or hardware key. SMS is no longer enough.

2. **Rewrite your wire-verification callback policy this week**
   Two people. Number from your system of record, not the email. Monthly challenge phrase.

3. **Set DMARC to p=reject on your sending domain**
   Stops most spoofed emails that pretend to come from you. 20-minute change.

4. **Run a 60-minute tabletop this quarter**
   Owner, finance, operations, outside counsel. Discover the gaps before an attacker does.

5. **Pull the SOC 2 and breach-notification clause for your top 5 vendors**
   If they can't produce either in a week, that tells you something.

REAL-WORLD CASE · HONG KONG · FEBRUARY 2024

Arup: $25 million wired off a single video call.

A global engineering firm, 18,000 employees, was taken in the largest documented deepfake fraud to date.

WHAT THE ATTACKERS DID

An entire video conference, faked.

- A finance employee in Hong Kong received an email about a "confidential acquisition" requiring urgent transfers
- Suspicious, the employee asked for a video call to verify
- The CFO and several familiar colleagues joined the Teams call — voice, face, mannerisms all matching
- Reassured, the employee authorized 15 transfers totaling US$25M
- Every executive on the call was an AI-generated deepfake. Real source material: prior public conference videos

WHAT WOULD HAVE STOPPED IT

An out-of-band verification policy, no exceptions.

- Independent call-back to a known phone number — never one provided in the request
- Mandatory two-person approval on wires above a low threshold (e.g., $25K)
- A standing rule: no single video or voice contact authorizes a transfer, period
- A monthly-rotating verbal challenge phrase known only to executives and finance

Sources: World Economic Forum (Feb 2025) · Reality Defender / WEF Global Cybersecurity Outlook 2025

REAL-WORLD CASE · UK · 2024

WPP: the attempt that failed because someone smelled it.

The world's largest advertising group, CEO Mark Read targeted by an AI-cloned-voice scam — and the attack was caught.

WHAT THE ATTACKERS DID

A perfect voice. A wrong context.

- Attackers set up a WhatsApp account using a public photo of CEO Mark Read
- Scheduled a Microsoft Teams meeting with a senior executive
- On the call, played a voice clone of Read — drawn from publicly available media — alongside YouTube footage
- Posed as Read soliciting personal details and money to set up a "new business"
- The targeted executive grew suspicious of the off-pattern request and reported it before any loss

WHAT MADE THE DIFFERENCE

Permission to be skeptical of the boss.

- A culture where employees are encouraged — and rewarded — for questioning unusual executive requests
- Awareness training that uses real cases, not generic phishing examples
- A clear, no-shame escalation path: "if it feels off, escalate it"
- Public-facing executives keep personal channels (WhatsApp, SMS) out of the financial approval workflow entirely

Source: The Guardian, May 2024 · WPP internal memo from CEO Mark Read

REAL-WORLD CASE · ITALY · JULY 2024

Ferrari: the question one executive asked that ended the call.

A flawless voice clone of the CEO — defeated by a single sentence of human verification.

WHAT THE ATTACKERS DID

The accent was perfect. The question was the test.

- A senior Ferrari executive received WhatsApp messages and a follow-up call from "CEO Benedetto Vigna"
- The voice clone reproduced Vigna's exact southern Italian accent — convincing on tone, cadence, and inflection
- The caller pressed for urgent help with a confidential currency-hedging transaction
- The executive grew uneasy at the slightly off context and asked Vigna a question only the real CEO would know
- The caller hesitated. The line went dead. No funds moved

THE COUNTERMEASURE

A pre-agreed verification question. Always.

- Establish a verbal challenge protocol for high-trust requests — known only to a small group, rotated quarterly
- Train executives and finance staff to ask, even when the voice is unmistakable: trust is not the same as verification
- Publish less. The fewer recordings of leadership voices in the wild, the harder the clone is to train
- If the request is genuinely urgent, the legitimate caller will answer the question without hesitation

Sources: Bloomberg, July 2024 · WEF "Detecting Dangerous AI" report (July 2025)

OVER TO YOU

Questions.

The best ones tend to be the ones you're afraid to ask in front of your team.

Brandon Lockett, CEO · Neutron Engineering
brandon.lockett@neutroneng.com · 443.606.0411 · oneneutron.com

Thank you.

Have a great rest of the summer — and a safer Monday.

Brandon Lockett, Chief Executive Officer
Neutron Engineering · Managed IT & Cybersecurity, built for businesses that run on trust

brandon.lockett@neutroneng.com · 443.606.0411 · oneneutron.com

BOOTH-ONLY SLIDES

Ninety days. Three phases. One team.

From handshake to measurable risk reduction without disrupting the day job.

DAYS 0 — 30

Assess & Stabilize

01

- Full discovery and risk assessment
- Immediate wins on MFA, backups, email
- SOC telemetry onboarded within 14 days

DAYS 31 — 60

Harden

02

- EDR deployed on every endpoint
- Identity hardening, privileged-access cleanup
- Policy & procedure documentation

DAYS 61 — 90

Optimize & Rehearse

03

- Tabletop incident-response exercise
- Vendor risk review on top-10 vendors
- Board-level reporting cadence established

A NO-COST INVITATION

Find your three biggest exposures before an attacker does.

A 45-minute working session with our team, exclusive to attendees of this summit. You leave with a prioritized short-list of the three issues most likely to cost you in the next twelve months — and what to do about each.

45 minutes

Virtual, no prep required from you

No obligation

You keep the findings either way

Delivered in 14 days

A written brief, not a sales deck

Find me at the Neutron table after this session · Brandon Lockett · brandon.lockett@neutroneng.com · 443.606.0411 · oneneutron.com

Why Neutron, and not the other logo on the booth table.

Five things that matter when the pager goes off at 2 a.m.

Built for regulated, finance-adjacent businesses

We speak FTC Safeguards, PCI, and cyber-insurance before the carrier asks.

24×7 US-based SOC

Humans on-shift, in-country, around the clock — not a chatbot and a voicemail tree.

One accountable partner

One throat to grab at 2 a.m. — not a finger-pointing chain of sub-vendors.

Examiner-ready documentation

Audit artifacts produced as a side effect of how we work — not a last-minute scramble.

Plain-English reporting

A monthly report a board of non-technical owners actually reads and acts on.