501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

A THANKSGIVING CYBER HEIST

How a Supply Chain Breach in QuickBooks Nearly Cost My Business $6,000

By Brian Scott, 501CISO

Introduction: A Holiday Season Cyber Surprise

I've spent most of my career in cybersecurity, and one of the universal truths of the field is that cyber incidents are spectacularly inconvenient. They don't arrive when you're sitting at your desk with your coffee. They don't wait until after the holidays. They arrive when you least expect them—on the evening before Thanksgiving, for example, just as you mentally transition from "business owner" to "I wonder how early is too early to slice the pumpkin pie."

And that is exactly when mine arrived.

This is the story of a supply chain attack—one executed through my accountant's compromised QuickBooks Online (QBO) access—that nearly resulted in a $6,000 loss for my small business. It's also the story of luck, timing, human intuition, and how one forgotten configuration saved me from becoming another cybercrime statistic.

But I'm not just telling the story. I'm using the **Incident Response Framework**—the same structured approach cybersecurity professionals rely on when everything goes sideways. Why? Because this framework turns chaos into clarity, and because it gives every organization—even the smallest cloud-based business—a blueprint for navigating the worst day of their digital year.

Why the Incident Response Framework Matters

The Incident Response lifecycle isn't academic. It isn't theoretical. It's a practical way to think your way through a crisis. It organizes the fog of emotion, adrenaline, and uncertainty into actionable steps.

And so, to show you *how to think* during an incident—not just what happened to me—I'm telling this story through these stages:

1. Detection & Analysis
2. Containment
3. Eradication
4. Recovery
5. Lessons Learned

Now let's begin where every breach story begins:
With the moment something feels… off.

1. Detection & Analysis — The Moment the Alarm Bell Rang

Thanksgiving Eve was peaceful. The house was quiet, the workday was behind me, and the holiday ahead promised a rare mental break. My wife, Courtney, was scrolling casually on her phone when she paused, frowned slightly, and said the words that changed everything:

"QuickBooks says you sent six bill payments this evening. Did you?"

In our house, QBO notifications are about as exciting as grocery-store coupons. Normally she swipes them away without a second thought. But not this time. This time she asked.

And that one question saved my business.

When I logged into QuickBooks Online, I felt an immediate jolt of wrongness. Six brand-new bills had been created. All were just under $1,000. All were queued for payment. All were designed to look routine enough to slip past a quick glance.

So I opened the audit log.

And that's when the timing revealed everything.

The attack didn't happen overnight or in the early hours of the morning, as so many brute-force attempts do. No, this happened at **5:01 PM**—the evening before Thanksgiving. A time when employees shut down their computers, offices close their doors, and support desks begin their long holiday slumber.

The bad actors knew exactly what they were doing.

Between **5:01 and 5:05 PM**, using my accountant's compromised QBO access, they:

- Logged into my tenant
- Edited multiple vendor ACH details
- Inserted their own banking information
- Created six fraudulent payments

Four minutes. That's all it took.

This wasn't guessing. This wasn't clumsy. This was a **precise supply chain attack**, executed by someone who understood QuickBooks' workflows and business behavior.

But here's the part that still gives me goosebumps.

Why did my wife get the notifications— and not me?

Years ago, when we set up QBO, Courtney helped me with light bookkeeping. At the time, it made perfect sense to list her email as the merchant account's primary contact. Over time, I took over all QBO work, and she stepped away. But like many legacy configurations, that setting remained exactly where it was.

And I forgot about it.

So when QuickBooks fired off six "Bill Payment Sent" emails, they went straight to Courtney's inbox—the only inbox in the world that would alert us in time.

If she had ignored them…
If we had been out of the house…
If her phone had been on silent…

I would never have known until the money was gone.

Sometimes cybersecurity hinges not on technology, but on a moment of human awareness.

And this was one of those moments.

2. Containment — "Freeze Everything!"

Once I confirmed the fraudulent bills, instinct took over. Cybersecurity professionals talk a lot about "containment"—the moment where you stop the bleeding before figuring out the cause.

For me, that meant grabbing my phone and calling my bank's fraud line immediately. The bank froze the business checking account on the spot. No money in. No money out. A total lockdown.

Which was exactly what needed to happen.

Next, I contacted my accountant—on Thanksgiving Eve—to deliver the awkward but necessary message:

"You've been compromised."

Then I opened a case with QuickBooks. With the immediacy of the situation, I expected some kind of rapid response.

But QBO, as I would soon learn, does not operate on adrenaline.

Thanksgiving dinner tasted a little different that night.

3. Eradication — Showing the Criminal the Door

The next step was to ensure the attacker could not reenter my environment.

Since the breach came through my accountant's access, the only option was immediate removal. I deleted their QBO connection entirely—cutting off the pathway the attacker had exploited.

When I finally reached their office the next day, they confirmed my suspicion:

I wasn't the only client affected. It's one thing to experience a cyber incident.
It's another to discover you were part of a larger, coordinated supply chain compromise.

And in that moment, the reality crystallized:

Even if your own systems are secure,
your partners' vulnerabilities can become your vulnerabilities.

Eradication removed the immediate threat but the aftermath was only beginning.

4. Recovery — The Two-Week Ordeal

Recovery is the longest, most grueling phase of incident response.

And in my case, it was a two-week odyssey that revealed more about QBO's internal processes than I ever wanted to know.

Immediately after I reported the fraud, QBO shut down my merchant account. That meant:

- No paying vendors
- No receiving payments
- No transferring funds
- No financial operations of any kind

My business was effectively frozen in amber.

The phishy email that wasn't phishing

One of the first emails QBO sent—requesting verification documents—looked so suspicious that we both assumed it was a scam:

- The layout was odd.
- The instructions were unclear.
- The "What We Need" section was blank.
- It emphasized clicking a mysterious link.
- And nothing about the incident appeared in my QBO dashboard.

If I were teaching a class on phishing, **that email would be Exhibit A**.

But it was real. And because we ignored it, my case stalled for days.

The daily ritual: Call QBO, hold, repeat

Every day, I called QBO's support line. Every day, I re-explained the story. Every day, the representatives read from the same script:

"Fraud will reach out."

They did not reach out.

The peak absurdity came when someone from the payments team finally called—completely unaware of the cyber incident—and informed me:

"You have a $6,000 balance. If you pay it, we can reinstate your account."

They wanted me to pay the exact amount the criminal had attempted to steal. Meanwhile, the Fraud team—the only team capable of resolving the incident—remained unreachable, uncontactable, and completely silent.

When Fraud finally called…

Nearly two weeks after the attack, the Fraud department finally reached out. And in that call, I learned something stunning:

The bad actor had, in fact, received the money.

QuickBooks BillPay operates on a "pay first, withdraw later" model. They sent the funds *out instantly*, and then attempted to pull reimbursement—from my bank account—after the fact. But because I had frozen my account, the withdrawal failed. So the criminal walked away with the money. And QuickBooks absorbed the loss. Not a dollar left my account, but the attacker succeeded. A surreal outcome, to say the least.

QBO told me they would "eat the cost," and reminded me—without irony—that "security of the account is ultimately the customer's responsibility."

I "gently" (maybe not so much) reminded them that:

- QBO does **not** allow admins to enforce MFA on all accounts
- QBO does **not** show MFA usage in audit logs
- QBO allows accountants broad access that mirrors client permissions
- This entire attack was possible because of *their* architectural limitations

They were polite but unmoved. I, on the other hand, was exhausted.

When they restored my merchant account, I went to the bank, unfroze the account, corrected the legacy email configuration, and finally—after two weeks—returned to normal operations.

5. Lessons Learned — What This Incident Really Revealed

By the end of this experience, I gained clarity on something cybersecurity professionals know but businesses rarely internalize:

Your security is only as strong as your weakest partner.

This breach reinforced for me:

- Supply chain risk is very real.
- QuickBooks' security controls are insufficient for modern threats.
- Audit logs without detailed data are incomplete logs.
- Vendor architecture choices directly affect customer risk.
- And communication breakdowns can extend business downtime far longer than any actual breach.

Most importantly:

My business was unable to pay bills for two full weeks, not because of the attack, but because of the recovery process.

That is the hidden cost of cybersecurity incidents:

- The time they require.
- The attention they demand.
- The operational paralysis they create.

Conclusion: One Glance Saved My Business

At the end of the day, everything came down to one quiet moment.

Courtney glanced at her phone. She noticed something strange. She asked a question. And that one glance—one that could easily have been missed—saved my business from losing $6,000.

Yes, a criminal stole money from QuickBooks. Yes, my business endured two weeks of operational friction. Yes, the failure came through a trusted partner. But it could have been so much worse.

Cybersecurity is not just firewalls and MFA prompts. It's a thousand tiny configurations, human habits, overlooked details, and moments of awareness that determine whether you experience a close call—or a catastrophe. If this can happen to a cybersecurity professional running a small

cloud business, it can happen to anyone. And the question isn't whether another supply chain attack will occur. The question is:

Will you detect it in time and will you be ready to respond?