

When Popular Solutions Don't Protect Your Business:

An \$800,000 Wake-Up Call

The Client

With fewer than ten employees handling significant government and commercial contracts, one Alberta-based service company (we'll call them 'HC') did what many growing businesses do: built their technology stack piece by piece, choosing well-known providers like GoDaddy for convenience and cost savings.

It worked out... for a while.

The Crisis

A routine follow-up on overdue payments was the beginning of a nightmare scenario. When HC nudged one of their biggest clients for the \$500,000 they were owed, the reply made their stomachs drop.

"We already sent it to that new bank account—just like you asked us to."

But HC had made no such request.

Cybercriminals had, in fact, breached their Microsoft 365 email system via their GoDaddy account and were impersonating the company, sending legitimate-looking banking change requests to their clients. We eventually discovered that over \$800,000 in expected payments had been redirected to fraudulent bank accounts.

Despite two weeks of attempting to resolve the breach through GoDaddy's standard support channels, the compromised accounts remained active. (So much for customer service, right?) The hackers continued to send fraudulent emails while the company watched helplessly.

Evolution's Response

Evolution IT was brought in as an emergency referral thanks to one of our existing clients. Our immediate priorities were clear:

Seal the Breach (First 24 Hours)

- Secured all compromised accounts and implemented proper access controls
- Deploy multi-factor authentication across all systems
- Conduct a comprehensive audit to identify the full scope of the breach

Damage Assessment & Investigation

- Discovered the second affected client during our forensic review
- Identified which customers had been contacted and what information was compromised
- Worked with HC to develop a communication strategy for affected parties

Incident Management Support

- Guided the client through law enforcement reporting procedures
- Advised on legal consultation for potential recovery actions
- Helped coordinate with insurance providers regarding coverage

Long-term Security Implementation

- Migrated HC away from consumer-grade hosting to enterprise-level phishing protection
- Implemented endpoint detection and response (EDR) solutions
- Established comprehensive backup and disaster recovery protocols
- Developed ongoing monitoring and maintenance as their managed service provider



The Outcome

The immediate threat was neutralized within 24 hours, something that hadn't been achieved in the previous two weeks.

While it took nearly a year of legal and administrative processes, the client was eventually made whole for the full \$800,000 loss.

More importantly, they now operate with enterprise-grade security measures that provide ongoing protection against future threats. They also periodically remind their clients about proper verification procedures—awareness of these was the only reason an additional HC client hadn't transferred funds after receiving the same fraudulent email.

The Moral of the Story

Consumer-focused solutions aren't always designed for what professional businesses need. When you're running a company with significant receivables, compliance requirements, or sensitive client relationships, you need more than a helpdesk. You need an IT support team that understands your specific risks and knows how to address them effectively.

An ounce of prevention truly is worth a pound of cure. While enterprise-standard security measures cost more than doing nothing, they're a fraction of the potential loss when things go wrong.

This client learned that lesson the hard way. Your business doesn't have to.



Contact Us

Evolution IT specializes in helping Calgary businesses implement appropriate security measures that match their risk profile and operational needs. If you're questioning whether your current IT setup is truly protecting your business, we'd be happy to provide a complimentary security review.



Your Business **Evolution**, Powered by IT.
evolution-it.ca

