



THE FINANCIAL FIRM'S GUIDE TO CYBERSECURITY

***Protect Your Clients. Protect Your
Reputation. Protect Your Firm.***

Brought to you by Borderland IT Solutions

TABLE OF CONTENTS

Introduction: Cybersecurity is No Longer Optional

03

Section 1: Top Cybersecurity Threats Facing Financial Firms

04

Section 2: The True Cost of a Cybersecurity Breach

05

Section 3: 7 Critical Steps to Protect Client Data
(Without Hiring a Full-Time IT Team)

06

Section 4: Why Borderland IT Solutions is the Partner of Choice for Financial Firms

08

INTRODUCTION

CYBERSECURITY IS NO LONGER OPTIONAL



In the last 10 years, financial firms have more and more become targets of cyber attacks.

Cyberattacks against wealth managers, accounting firms, and financial advisors have increased by over 68% year-over-year.

Why? Because criminals know that financial firms are smaller targets than banks – but often hold just as much valuable data.

Without a strong cybersecurity plan, your firm could face:

- Financial devastation
- Regulatory penalties
- Loss of client trust
- Permanent brand damage

The hard truth: It's no longer a question of if you'll be targeted. It's a question of when.

And when that day comes, will you be ready?

Borderland IT Solutions specializes in helping financial firms like yours build battle-tested defenses without the cost or complexity of hiring an in-house IT team.

This guide shows you how to stay protected – and how to turn cybersecurity from a liability into a competitive advantage.

SECTION 1

TOP CYBERSECURITY THREATS FACING FINANCIAL FIRMS IN 2025

Threat	What It Means	Example
Phishing & Spear Phishing	Highly targeted emails that trick staff into clicking malicious links or revealing credentials.	An email posing as your custodian asks your admin to "verify" client data – but it's a trap.
Ransomware	Criminals encrypt your data and demand payment to unlock it.	Your bookkeeping files are encrypted during tax season – right when you need them most.
Business Email Compromise (BEC)	Criminals hijack internal email to authorize fake wire transfers or transactions.	A "client" emails from a compromised account asking for a last-minute \$150,000 wire.
Third-Party Vendor Risk	Your software providers or outsourced partners become entry points for hackers.	Your outsourced payroll processor gets breached, exposing your client PII.
Regulatory Compliance Failures	Failing audits or security standards leads to fines, lawsuits, and reputation loss.	A FINRA audit reveals inadequate encryption of stored client documents, triggering penalties.

Key Insight:

Financial firms are increasingly judged not just by performance, but by their ability to protect sensitive data.

Cybersecurity is now a core pillar of client trust.

SECTION 2

THE TRUE COST OF A CYBERSECURITY BREACH



Beyond the immediate ransom payment or downtime, a breach can cripple your business long-term:

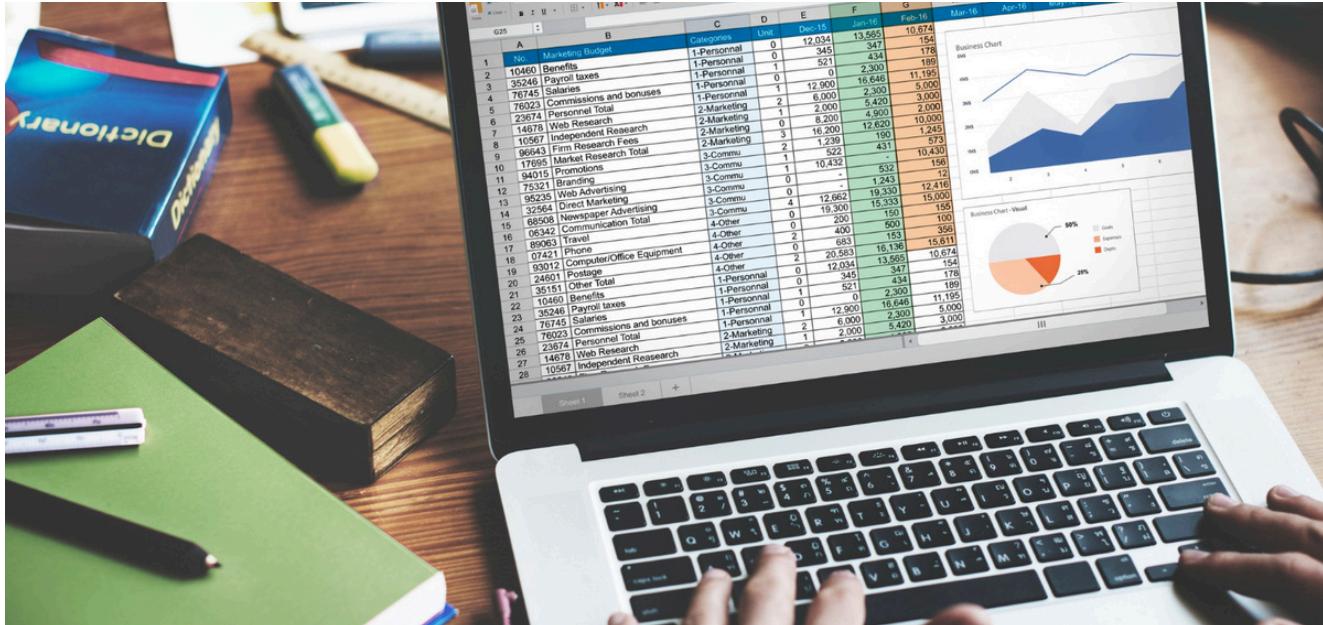
- Average Cost of a Breach: \$4.45M (IBM 2024 Cost of a Breach Report)
- Client Loss: 67% of clients would leave after a cybersecurity incident (Ponemon Institute)
- Fines and Penalties: SEC enforcement actions and private lawsuits cost firms an average of \$1.2M
- Downtime: Average breach downtime is 21 days – and recovery often takes months.
- Reputational Damage: Negative press can destroy your ability to win new business for years.

One firm we assisted had a breach traced back to an unprotected Dropbox folder.

They spent \$85,000 on legal fees alone – before we even started the remediation work.

SECTION 3

7 CRITICAL STEPS TO PROTECT CLIENT DATA (WITHOUT HIRING A FULL-TIME IT TEAM)



1. Implement Multi-Factor Authentication (MFA) Everywhere

- A simple password isn't enough.
- MFA blocks 99.9% of account takeover attempts.

2. Encrypt All Data — In Transit and At Rest

- Secure email platforms and encrypted storage solutions are essential.
- Compliance requires it, but so does common sense.

3. Ongoing Security Awareness Training

- Your employees are your biggest risk and your best defense.
- Short, regular trainings drastically reduce phishing click rates.

4. Advanced Endpoint Protection

- Install next-generation antivirus and EDR (Endpoint Detection & Response) tools.
- Cover every laptop, desktop, tablet, and mobile device.

5. Conduct Regular Cybersecurity Risk Assessments

- Discover vulnerabilities before the hackers do.
- Annual or semi-annual assessments are a compliance best practice.

6. Backup Data Daily (and Test Your Recovery)

- Air-gapped, encrypted backups are critical.
- Regular backup tests ensure you can restore quickly after an incident.

7. Partner With a Specialized MSP

- Gain the benefit of 24/7 monitoring, rapid incident response, and compliance expertise.
- A fraction of the cost of building an internal team.

SECTION 4

WHY BORDERLAND IT SOLUTIONS IS THE PARTNER OF CHOICE FOR FINANCIAL FIRMS

When you choose Borderland IT Solutions, you're not just hiring an IT provider — you're gaining a strategic ally who understands the stakes in the financial world.

Here's what sets us apart:

Financial Industry Focus

We understand SEC, FINRA, NYDFS, IRS, and HIPAA standards inside and out — and help you meet them without the jargon.

Customized Cybersecurity Plans

No cookie-cutter security bundles. Every engagement starts with a full assessment and a tailored strategy.

Real-Time Threat Monitoring

Our Security Operations Center (SOC) monitors your systems 24/7/365 to detect and neutralize threats in real time.

Compliance Support

We provide audit preparation, policy development, and compliance reporting — so you stay ahead of regulatory demands.

Fixed Monthly Pricing

No surprises, no nickel-and-diming. Just predictable, manageable costs.

ACT NOW — PROTECT YOUR CLIENTS, YOUR FIRM, AND YOUR FUTURE

Cybercriminals are not waiting. Every day that passes without taking action increases your exposure — and the potential cost.

Don't wait for a breach to make cybersecurity a priority.

Get ahead of the risks today, with a partner who understands financial firms inside and out.

Here's what to do next:

Step 1: Book a complimentary 30-minute IT Systems Evaluation with Borderland IT Solutions

Step 3: Walk away with a customized action plan — at no cost, no commitment.

(Spots are limited each month to ensure high-touch service — book early!)

SCHEDULE MY FREE EVALUATION



915-229-8787



borderland-it.com



info@borderland-it.com

Protect your firm today. Sleep better tonight. Build client trust forever.
Borderland IT Solutions is here to help you every step of the way.