WHY DIGITAL DEFENSE? YOUR BUSINESS, SECURED.

FRANCELL FLOOD, CISM, CCSP, CYSA+
INTERNATIONAL BUSINESS CYBERSECURITY CONSULTANT | AUTHOR | SPEAKER

ABOUT US

International Business Cybersecurity Consultant | Author | Speaker

Our Mission: To translate complex cyber threats into simple, actionable steps designed specifically for your small business.

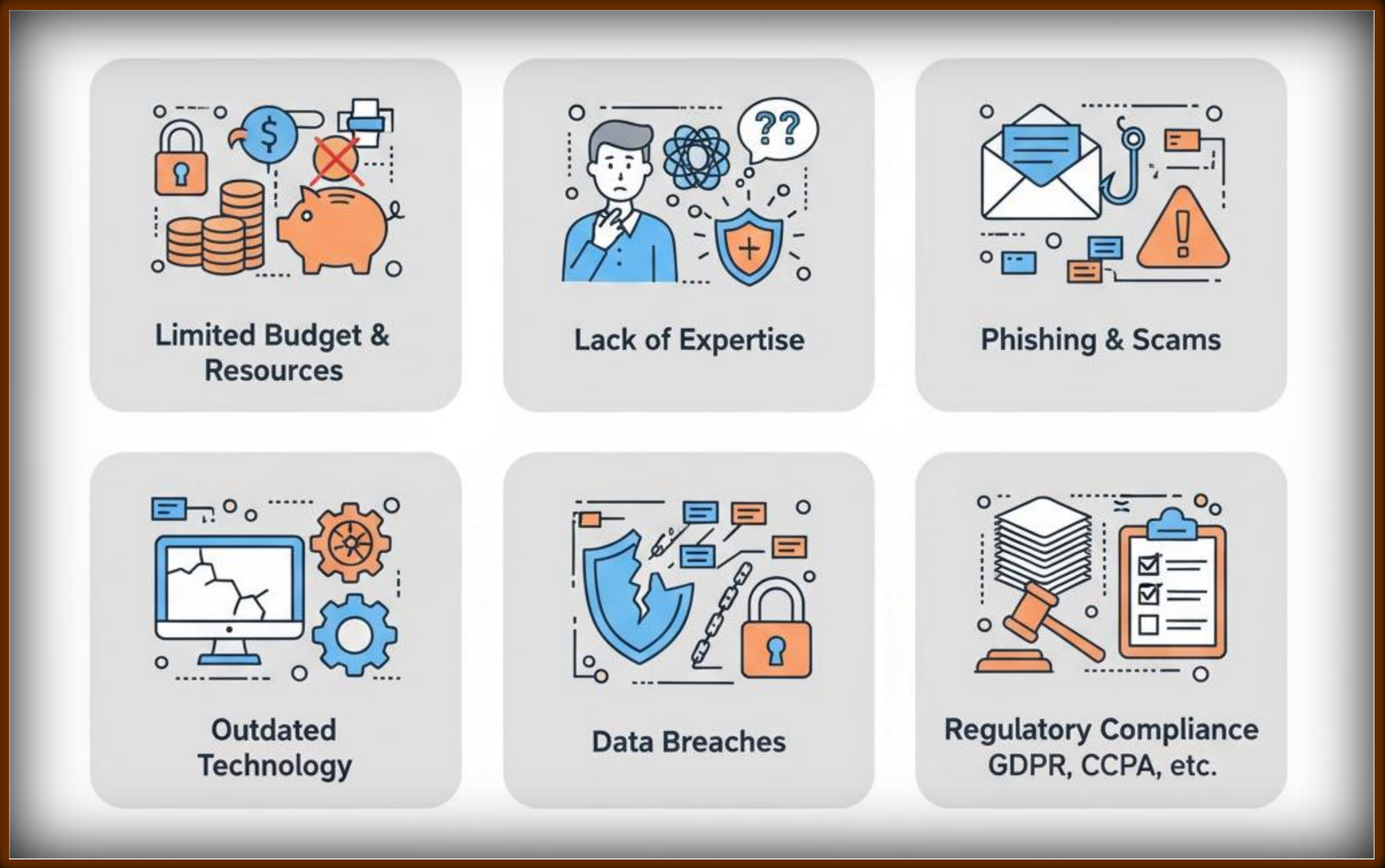
Our experience as International Business Cybersecurity Consultants spans ten years while our qualifications enable us to convert complicated security threats into useful business strategies. Our expertise enables you to understand technical concepts which we transform into business friendly solutions that protect your organization from threats while maintaining regulatory compliance.

COMPANY OVERVIEW

“IF YOU CAN'T EXPLAIN IT SIMPLY, YOU DON'T UNDERSTAND IT WELL ENOUGH.”

- I founded this company because I saw that small and medium-sized businesses, the backbone of our economy, were being left dangerously exposed to cyber threats. Small businesses account for about **43.5% of the U.S. economy's GDP** and employ approximately **45.9% of American workers.** Source
- Many small businesses are unable to afford or understand the complex solutions built for large corporations. My mission is to close that critical gap by delivering **straightforward, actionable cybersecurity strategies** that busy business owners can actually implement and understand. Public speaking isn’t just marketing tool, but a critical platform to demystify the threat landscape, strip away technical jargon, and directly empower hundreds of people with the essential knowledge needed to protect their assets and their customers.

PAIN POINTS OF SMALL BUSINESSES



PROBLEM

- **Market Gap**: Most Cyber Security Solutions are made for companies with large budgets. Small businesses are prime targets, often without dedicated IT security. Threats are complex, but solutions don't have to be.
- **Per Year Cost**: Small businesses (1-250 employees) in North America spend an average of **$2,500 per month** on cybersecurity, equating to **$30,000 annually** Source
- **Costs**: Each breach. At the low end, the average cost of a cyberattack for small businesses was **around $120,000 to $200,000.** Source
  At the high end, organizations with **fewer than 500 employees**, the average cost of a data breach in 2023 was **$3.31 million USD.** Source
- **Usability**: businesses want something easy to use that helps make their life easier

KEY CLIENT OUTCOMES

How Can We Help You?

SERVICE PORTFOLIO

- **Foundational Cybersecurity Services (Core Protection) - Essential services to establish immediate and robust security.**
- **Empower Your Team, Strengthen Your Walls (Proactive Defense) - Transforming your staff into your strongest defense.**
- **Navigating the Landscape (Strategy & Compliance) - Protecting your reputation and navigating regulatory requirements.**
- **Trusted Cybersecurity Partner (Ongoing Support) - Continuous expertise without the full-time cost.**

FOUNDATIONAL CYBERSECURITY SERVICES (CORE PROTECTION)

Step 1: Cybersecurity Quick-Scan & Risk Assessment

Description: Identify your top 3-5 immediate cyber risks, vulnerabilities, and compliance gaps.

Output: Simplified "Risk Report" with prioritized, actionable recommendations.

- **Overall View**
- **High Ticket Items**
- **Report for condensed targeted focus**

Step 2: "Secure Start" Baseline Setup

Description: Guided assesment of essential controls: strong passwords, MFA, basic firewall, secure Wi-Fi.

Output: Hardened security baseline for critical systems.

- **Baseline Security**
- **Basic Cyber Hygiene**
- **Baseline Hardening makes unattractive targets**

Essential services to establish immediate and robust security.

FOUNDATIONAL CYBERSECURITY SERVICES (CORE PROTECTION)-CONTINUED

Step 3: Data Backup & Recovery Plan

Description: Design and lay out a simple, effective 3-2-1 backup strategy and recovery checklist.

Output: Ensuring business continuity and rapid resilience against data loss.

- **Data always accessible**
- **Data is replicated and secure**
- **Customer data protections**

Step 4: Proactive Defense & Awareness

Description: Scanning for vulnerabilities in the infrastructure.

Output: Reviewing hardware and looking for End-of-Life (EOL) devices.

- **Less vulnerabilities means less attack vectors**
- **Inventory of all devices and software**
- **Less EOL Hardware, less attack vectors**

EMPOWER YOUR TEAM, STRENGTHEN YOUR WALLS (PROACTIVE DEFENSE).

Step 5: Employee Cybersecurity Awareness Training (Non-Technical)

Description: Interactive workshops (online/in-person) on phishing, ransomware, secure browsing, and data handling.

Output: Training materials, quizzes, and certificates.

- **Humans are your weakest link**
- **Frequent, short sessions are more effective**

Step 6: Phishing Simulation & Training

Description: Conduct simulated phishing campaigns, identify vulnerabilities, and provide targeted training.

Output: Building a strong "human firewall" against top threats.

- **Security mindset in each employee saves time and money.**
- **Instills a sense of responsibility**

Step 7: Secure Remote Work Setup

Description: Guidance for securing remote access, cloud tools, and employee devices.

Output: Adapting operations safely to modern, flexible work environments.

- **Working Flexibility**

Transforming your staff into your strongest defense.

NAVIGATING THE LANDSCAPE (STRATEGY & COMPLIANCE)

Step 8: Cybersecurity Policy & Procedures Development

Description: Creation of essential, easy-to-understand policies (e.g., acceptable use, incident response, password policy).

Output: Personalized, clear documentation for internal use and compliance.

- **Continuity of Operations**
- **Less time onboarding new employees**

Step 9: Vendor / Third-Party Risk Assessment (Simplified)

Description: Framework and checklist to evaluate key vendors' cybersecurity posture.

Output: List of all supply chain risks and mitigations.

- **Supply Chain Attack responses**

Step 10: Incident Response Planning (Playbook Lite)

Description: Simplified "What to Do When..." playbook for common incidents.

Focus: Minimizing damage, downtime, and reputational harm after an attack.

- **Incidents will happen. Simple guide to avoid paralysis and actionable steps to follow.**

Protecting your reputation and navigating regulatory requirements.

TRUSTED CYBERSECURITY PARTNER (ONGOING SUPPORT)

Description: Ongoing advisory, quarterly check-ins, and on-demand support for strategy, vendor reviews, and threat intelligence.

Output: Providing continuous, expert guidance and peace of mind without the cost of a full-time CISO.

- **Fractional CISO cost less yet still have key input on Cyber Security issues.**
- **Working relationship so the infrastructure does not have to be explained to multiple vendors.**
- **Compliance and Security cost less than contracting out to a new auditor each year.**

Continuous expertise without the full-time cost.

THANK YOU

Francell Flood
301-310-9981
contact@francellflood.com
www.francellflood.com