

2025

FIR

FRAUD INTELLIGENCE REPORT

**OUTSMARTING FRAUD: EXECUTIVE PRIORITIES FOR
SMALL AND MID-SIZED BUSINESSES**

FIRRISKADVISORY.COM

MAY -2025

Fraud Intelligence Report (**FIR**) year 2: Over the past year, I've researched and published 52 newsletters focused on identifying the most reliable and useable open-source information about Cybersecurity trends, best practices and cyber-fraud. My objective for this **second edition report** is to educate small and mid-sized business leaders about the current state of cyber fraud and how this can cost your business profitability due to lost time and fees, stolen product, stolen intellectual property, stolen data and damage to your reputation. Threat actors are financially motived to commit cyber fraud as the marketplaces for stolen data, assets, and identities is extensive and built to reward those who can provide the inputs to easily and quickly access user accounts, transact on e-commerce platforms to test stolen payment cards, commit payment fraud, and abuse free trial programs. We present the **big picture** about the current fraud threat landscape, **risk vectors** that fraudsters commonly abuse, and **cybersecurity news** to keep you informed of recent trends.

We wrap up with **key takeaways** to help you stay vigilant in protecting your business.

Empowering businesses to outsmart fraud!



Bruce Bird, Principal, FIR Risk Advisory LLC

TABLE OF CONTENTS

| | |
|-----------------------------------|----|
| BIG PICTURE | 3 |
| TOP RISK VECTORS/ ATTACK TRENDS | 7 |
| ATTACKS AND ATTACKERS MAKING NEWS | 10 |
| HOW TO PROTECT YOUR BUSINESS | 11 |
| ARTIFICIAL INTELLIGENCE | 13 |
| ABOUT FIR RISK ADVISORY | 19 |
| RESOURCES | 20 |

BIG PICTURE

In 2025, cyber-fraud continues to escalate as attackers exploit vulnerabilities, misconfigurations, and human error with increasing sophistication. This report synthesizes insights from many leading cybersecurity sources to provide a comprehensive view of the threat landscape and actionable strategies for organizations of all sizes. This year's edition is focused on small and medium-sized business (SMB) in general, but as you will see, this report can be applied to any organization as attackers are following the path of least resistance most often, which places SMB organizations squarely in the sights of the adversaries, who motives are exclusively financial and run by organized crime syndicates.

I've also incorporated other sources (see Resources section) that I have used in my weekly FIR Risk Newsletter series to supplement this year's report with added insights.

2025 STATISTICS AND INSIGHTS:

2025 marks an inflection point in cyber and fraud risk. Small and mid-sized businesses (SMBs) face unprecedented threats, with attackers shifting tactics to identity fraud, payment fraud, supply chain exploitation, and operational disruption via ransomware and deepfake-enabled social engineering.

KEY STATISTICS:

- **79%** of attacks are malware-free (CrowdStrike 2025)
- **86%** of incidents involve operational disruption (Unit42 2025)
- **30%** of total intrusions involve identity-based attacks (IBM X-Force 2025)
- Cloud and SaaS compromises surged by **29%** (Unit42 2025)
- Third-party breaches **doubled** year-over-year (Verizon DBIR 2025)

INSIGHT #1: FRAUD IS FASTER, MORE TARGETED, AND INCREASINGLY AI-POWERED.

INSIGHTS

- **Exploits** are the top initial infection vector, driving **33%** of breaches (Mandiant).
- **Manufacturing** is the most targeted industry, facing **26%** of attacks (IBM).
- Global median **dwell time** rose to **11 days** (Mandiant), while **Unit42** reports a decrease to **7 days** in some regions.
- **Ransomware** was involved in **21%** of incidents (Mandiant), with **28%** of malware cases linked to ransomware (IBM).
- **Data theft** occurred in **37%** of cases (Mandiant), with **credential theft** rising by **12%** (IBM).
- **Insider threats** from North Korean IT workers contributed to **5%** of initial vectors (Mandiant), with a **tripling** of cases tied to North Korea (Unit42).
- **Phishing** reclaimed its spot as a leading vector, accounting for **23%** of breaches (Unit42).

Attackers leverage info-stealer malware, unsecured data repositories, cloud misconfigurations, and AI-assisted tactics. Defenses must prioritize MFA, patching, employee training, and proactive threat detection.

INSIGHT #2: CREDENTIAL THEFT IS ALLOWING THE ADVERSARY TO ACCESS ACCOUNTS AT WILL!

INSIGHT #3: EXPLOITATION OF KNOWN VULNERABILITIES GIVES THE ADVERSARY A HEAD START AND CLEAR PATHWAY INTO YOUR COMPANY'S INFRASTRUCTURE AND APPLICATIONS.

Initial Infection Vector, 2024



Mandiant M-Trends 2025 Report, page 10

Figure 1 below: Initial Infection Vectors, Mandiant M-Trends 2025

This chart displays the distribution of initial infection vectors, with exploits at 33%, stolen credentials at 16%, and phishing at 14%.

THE 2025 CYBERCRIME LANDSCAPE REFLECTS SEVERAL PIVOTAL SHIFTS:

- **Info-stealer Malware Surge:** Credential theft fuels breaches, with stolen credentials at **16%** of vectors (Mandiant) and a **12%** increase in dark web sales (IBM).
- **Unsecured Data Repositories:** Poor security hygiene exposes data in tools like SharePoint and GitHub (Mandiant).
- **Cloud Migration Risks:** Misconfigurations and weak identities widen attack surfaces, with **29%** of cases involving cloud environments (Unit42).

- **AI-Assisted Attacks:** Attackers use AI to scale phishing and malware, with a **doubling** of synthetic text in malicious emails (Verizon).
- **Third-Party Involvement:** Breaches involving third parties doubled to **30%** (Verizon).
- **Insider Threats:** North Korean IT workers infiltrate organizations, posing risks of data theft and extortion (Mandiant, Unit42).

These trends demand a data-centric security focus, emphasizing visibility, access control, and proactive threat management.

INSIGHT #4: WEAK IDENTITIES WIDEN ATTACK SURFACES.

INSIGHT #5: THIRD PARTY VENDOR RISK MANAGEMENT IS REQUIRED.

Figure 2: Third-Party Involvement in Breaches, Verizon 2025 DBIR

This party-themed glyph chart depicts a doubling of third-party involvement in all breaches analyzed to 30%, driven by vulnerability exploitation.



Figure 10. Percentage of third-party involvement in breaches (each glyph is 2%)

Verizon DBIR Data Breach Investigations Report, page 15

TOP RISK VECTORS/ ATTACK TRENDS

TOP 5 DETAILED FRAUD THREATS

1. Ransomware and Extortion

- ✿ *Description:* Attackers encrypt data and threaten leaks, with ransomware in **21%** of incidents (Mandiant) and **28%** of malware cases (IBM).
- ✿ *Impact:* Median dwell time for adversary-notified cases is **5 days** (Mandiant), with extortion demands rising by **80%** (Unit42).

Figure 3: Ransomware Trends Over Time, Verizon 2025 DBIR

A line graph showing a 37% increase in ransomware involvement in breaches compared to the previous year.

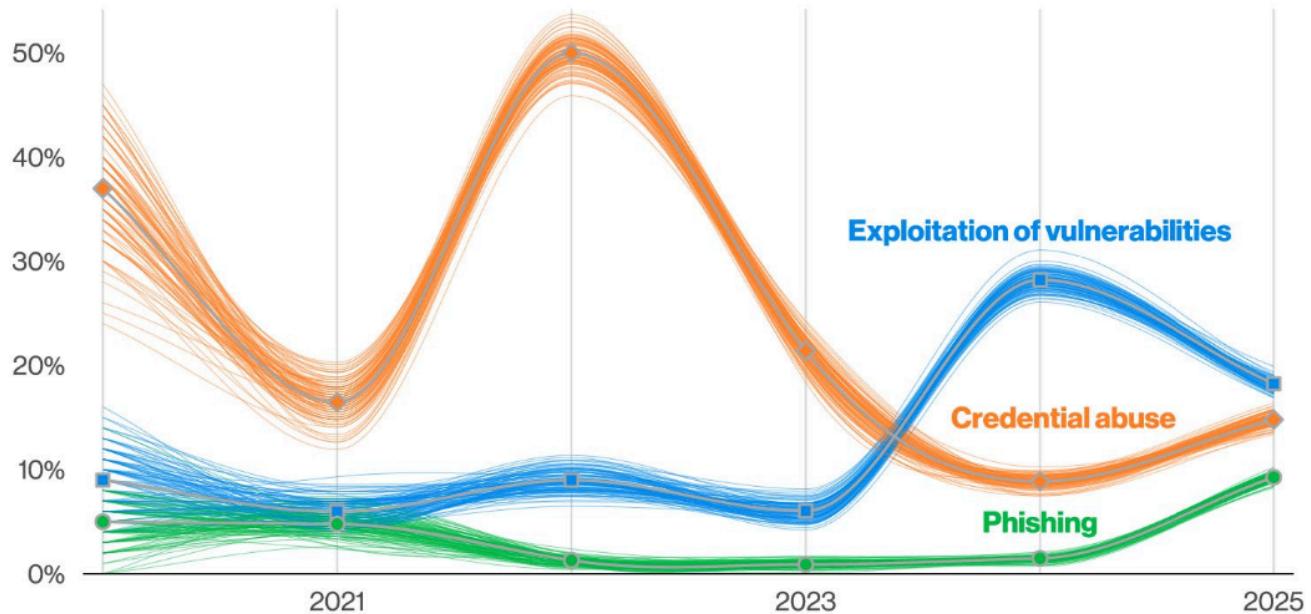


Figure 45. Known initial access vectors over time in Ransomware action breaches (n in 2025 dataset=4,630)

Verizon DBIR Data Breach Investigations Report, page 40

2. Info-stealer Malware

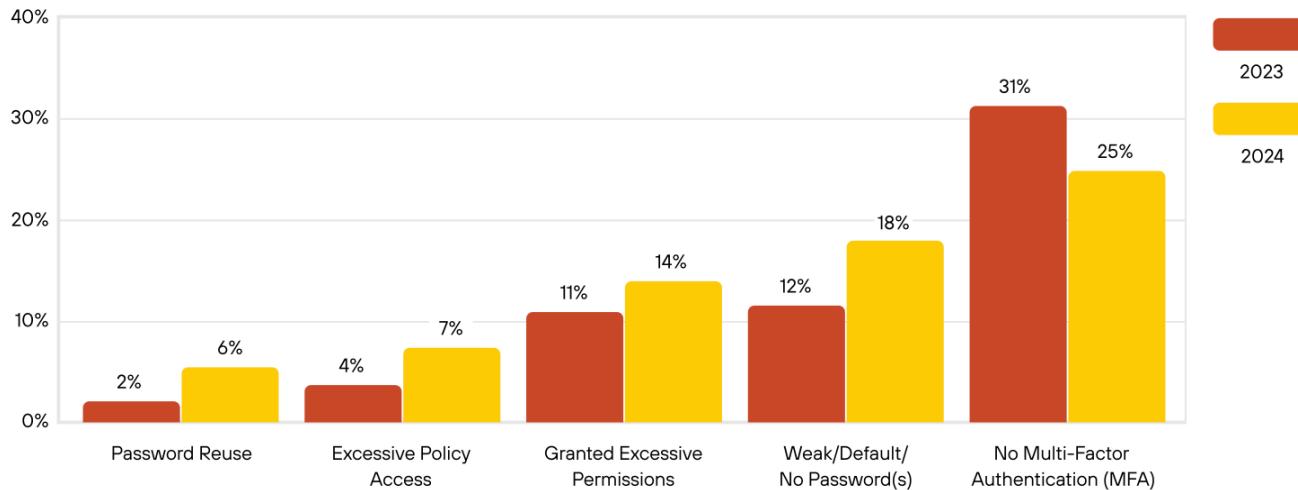
- ✿ *Description:* Malware harvests credentials, enabling access and lateral movement (**16%** of vectors, Mandiant). Once installed, info-stealers run in the background to take screenshots, capture keystrokes, access passwords, and compromise financial and personal information without user knowledge (IBM X-Trends 2025).
- ✿ *Impact:* Fuels follow-on attacks, with an **84%** rise in info-stealers via phishing (IBM).

3. Cloud Compromises

- ✿ *Description:* Misconfigured cloud systems and weak identities are exploited, with **29%** of cases involving cloud (Unit42).
- ✿ *Impact:* IAM issues contributed to **41%** of incidents (Unit42).

Figure 4: Cloud-Related Incidents, Unit42 Global Incident Response Report

A bar chart illustrating trends in identity and access management issues from 2023 to 2024.



Unit42 Global Incident Response Report Figure 2, page 11

4. AI-Powered Attacks

- ✿ *Description:* AI scales phishing and malware evasion, with synthetic text in emails doubling (Verizon).
- ✿ *Impact:* Simulated attacks show AI reducing exfiltration time from **2 days** to **25 minutes** (Unit42).

5. Insider Threats

- ✿ *Description:* Deceptive employees steal data or extort firms (**5%** of vectors, Mandiant).
- ✿ *Impact:* Cases tied to North Korea tripled in 2024 (Unit42).

Figure 5: Adversaries increasingly adopted genAI throughout 2024, Crowdstrike Global Threat Report 2025

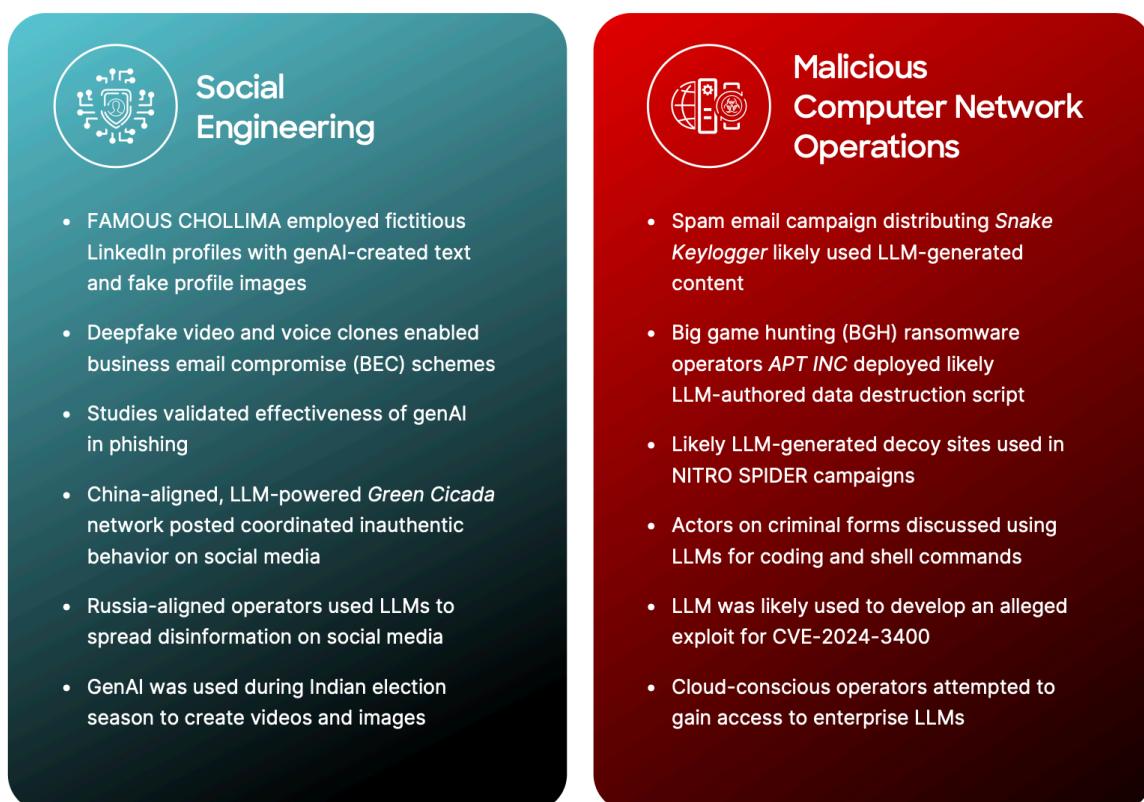


Figure 8: Adversaries leveraging LLMs for social engineering and malicious CNO

ATTACKS AND ATTACKERS MAKING NEWS

ATTACK SNAPSHOTS

- **Volt Typhoon (UNC5135):** Chinese espionage group infiltrating U.S. critical infrastructure, recently exploited Ivanti Connect Secure VPN vulnerabilities for persistent access (Mandiant).
- **MOVEit Exploitation:** Widespread third-party data theft via MOVEit software vulnerabilities impacted thousands of global organizations (Verizon).
- **Snowflake Compromise:** Misconfigurations in Snowflake cloud platforms enabled unauthorized data exfiltration, stolen credentials abused to access SaaS platforms (Unit42).
- **BlackCat (ALPHV):** Ransomware group UNC3944 used stolen credentials and exploits for encryption and extortion attacks (Mandiant).
- **Palo Alto Networks PAN-OS (CVE-2024-3400):** Zero-day exploit led to ransomware deployment by a RANSOMHUB affiliate (Mandiant). Palo Alto Networks PAN-OS could allow a remote attacker to execute arbitrary command on the system, caused by a command injection vulnerability in the GlobalProtect feature. An attacker could exploit this vulnerability to inject and execute arbitrary code on the system with root privileges. (IBM X-Trends 2025).
- **CURLY SPIDER** emerged as one of the fastest and most adaptive eCrime adversaries, executing high-speed, hands-on intrusions. In this case, the adversary attempted to achieve their objectives without even needing to break out to another device. The entire attack chain — from initial user interaction and social engineering to introducing a backdoor account to establish persistence — took under four minutes. (CrowdStrike Global Threat Report 2025).

These incidents highlight diverse tactics, from exploits to insider threats, underscoring the need for comprehensive defenses.

HOW TO PROTECT YOUR BUSINESS

ACTIONABLE DEFENSE MOVES FOR SMB'S

Small and medium-sized businesses (SMBs) cannot match attackers' resources, but with smart prioritization, faster response capabilities, and strategic partnerships, they can dramatically reduce fraud and cyber disruption risk. Bolster security with these practical steps:

- **Identity Protection First:** Mandate MFA and least privilege access across all systems, especially cloud and remote access (Mandiant, Unit42, Crowdstrike).
- **Be Prepared:** Establish rapid incident response playbooks and pre-arrange cybersecurity Incident Response services (retainer model).
- **Educate Employees:** Train on phishing, social engineering, deepfakes and data handling (Verizon).
- **Protect Endpoints and Monitor Activity:** Deploy endpoint detection tools to spot anomalies (Unit42).
- **Secure Cloud and SaaS Systems:** Use least privilege, encryption, and audits for hybrid environments (IBM).

5 "DO NOW" ACTIONS (QUICK WINS)

1. **Enable MFA:** Protect against credential theft immediately by enabling phishing-resistant MFA across email, cloud, and finance systems (Mandiant, Unit42, Crowdstrike).
2. **Patch Systems:** Address critical vulnerabilities in security devices (Mandiant).
3. **Run Phishing Simulations:** Boost employee awareness swiftly (Verizon).

4. **Audit Access:** Restrict permissions to sensitive data, conduct privileged access audits to verify users who have elevated privileges across critical systems (IBM).
5. **Backup Data:** Backup mission-critical data offline and test restores to counter ransomware (Unit42).

5 "STRATEGIC WATCH TRENDS" (FUTURE-PROOF PLANNING)

1. **AI-Powered Attacks:** Expect AI-driven phishing and malware evasion (Unit42, Verizon).
2. **Ransomware Evolution:** Multi-extortion tactics will intensify (Mandiant, Unit42).
3. **Cloud Security Gaps:** Misconfigurations will remain a prime target (Unit42, IBM).
4. **Insider Threat Growth:** Beyond DPRK, insider risks will rise (Mandiant, Unit42).
5. **Data-Centric Focus:** Enhanced data protection will be critical (Mandiant, Verizon).

INSIGHT #6: INVESTIGATE PHISHING RESISTANT PASSWORD-LESS TECHNOLOGY.

INSIGHT #7: EXPECT TO BE ATTACKED AND PREPARE YOUR RESPONSE PLAN.

INSIGHT #8: KNOW YOUR DATA, WHERE IS IT, AND HOW ITS PROTECTED.

INSIGHT #9: EDUCATE YOUR TEAMS, HELP THEM STAY VIGILANT.

INSIGHT #10: KNOW YOUR INFRASTRUCTURE AND 3RD PARTY DEPENDENCIES.

ARTIFICIAL INTELLIGENCE

Last year, when I wrote my first edition FIR, the AI capabilities were not nearly good enough to rely on for any credible information. In April 2024, when I queried ChatGPT for example (or any of the LLMs from Google, Meta, X.AI, or Anthropic), the best these models could do was basic grammar checking and maybe give suggestions on sentence structure. But, when it came to actual cybersecurity information, they were all very poor and mostly “made up stuff”, including sources, if you took the time to fact check them, which I did.

One year later, AI is now performant, very accurate (especially if you learn how to ask it questions), and if you use the reasoning models, they are very good at problem solving. At the end of the day, problem solving is what Cybersecurity and Fraud Prevention is all about, how do we keep the adversary out of our business, how do we protect against all the fraudulent activity, the scams, the card testing, the hacking of user accounts, the abuse of our promotions, or the theft of our crown jewels. As a test, I’ve decided to include AI’s response to the following question:

Q: I’m a small e-commerce business owner and don’t have the people or budget to manage cybersecurity and fraud prevention risks for my company, what should I do to improve my security posture?

Here’s what Grok-3 delivered:

I understand your resource constraints. Let’s simplify to the essential must-do steps to protect your small e-commerce business right now, focusing on immediate impact with minimal time and cost. These prioritize the most critical risks—ransomware, data theft, and fraud—given your online-only operation.

ESSENTIAL STEPS TO TAKE NOW

- 1. Secure Your Website and Transactions.** Ensure your site uses HTTPS (check for a padlock in the browser). If not, get a free SSL certificate (e.g., from Let’s Encrypt). Confirm your payment processor or marketplaces handle encryption; if not, switch to one that does (e.g., PayPal, Stripe). Cost: Free or minimal (included with most hosts).

- 2. Enable Multi-Factor Authentication (MFA).** Turn on MFA for all employee emails, admin accounts, and marketplace logins. Use apps like Google Authenticator or text codes. Takes 1-2 hours to set up for your team. Cost: Free with most platforms.
- 3. Set Up Basic Backups.** Back up customer data, inventory, and financial records to an external hard drive or encrypted cloud (e.g., Google Drive). Do this weekly. Test restoring once to ensure it works. Cost: \$50-\$100 for a drive, or free with existing cloud storage.
- 4. Train Your Team on Phishing.** Use a 1-hour free online course (e.g., from CISA.gov) to teach your customer service team to spot phishing emails and fake transactions. Reinforce monthly with quick 15-minute reviews using real examples. Cost: Free.
- 5. Create a Basic Response Plan.** Write a one-page guide: disconnect affected devices, contact your bank/marketplace support, and notify customers if data is at risk. Share with your team and review it once in the next month. Cost: Free, just your time.

Why These Matter

These steps address the top threats: unsecured sites invite malware, weak logins enable theft, no backups cripple you against ransomware, phishing targets your team, and a response plan limits damage. They leverage your customer service team's skills and require minimal investment (\$50-\$100 upfront, mostly your time).

Here's what Chat-GPT 03-mini reasoning model had to say:

PHASE 0—RIGHT NOW (FIRST 30 DAYS)

These are “no-regrets” moves that cost little but block the attacks most small e-commerce firms actually suffer.

- 1. Name an owner for security and fraud.** Even if it's a part-time hat you wear yourself, someone must coordinate tasks and be the first call when something looks off. CISA's Cyber-Essentials calls this “Develop the Culture”.

- 2. Inventory what you must protect.** List laptops, phones, POS tablets, cloud services (Shopify, Amazon Seller Central, payment gateways, Gmail/Microsoft 365, QuickBooks, etc.). A simple spreadsheet works and becomes the backbone for patching, credential reviews, and insurance questionnaires. CIS Controls v8.1 put asset management at the very top.
- 3. Turn on MFA everywhere, starting with email, payment portals, and marketplace logins.** Stolen passwords remain the #1 entry point for small businesses. MFA stops more than 90% of automated takeover attempts. NordLayer's 2025 checklist places MFA in its first five items.
- 4. Adopt a password-manager and kill shared spreadsheets of passwords.** This is the cheapest way to get long, unique credentials without staff "recycling" the same one.
- 5. Patch all operating systems and critical apps.** Auto-update Windows/macOS, browsers, plugins, and any self-hosted web components.
- 6. Deploy modern endpoint protection (AV/EDR) on every device** and enforce full-disk encryption on laptops/phones that leave the office.
- 7. Back up business-critical data using the 3-2-1 rule** (three copies, two media, one offline or immutable). Test a restore before you need it—ransomware crews still rely on untested backups.
- 8. Launch basic employee security awareness training.** Use the free 30-minute videos and phishing simulation kits from NIST's Small Business Cybersecurity Corner.
- 9. Create a one-page incident-response cheat-sheet.** List who to call (payment processor, hosting provider, cyber-insurance, attorney), where backups live, and how to shut down order processing if needed.

How to keep momentum

- 1. Quarterly reviews** of the roadmap; tick off completed items, assign next owners.
- 2. Metrics that matter:** % MFA coverage, patch latency, failed fraud-rule counts, backup restore time, training completion rate.

3. **Celebrate quick wins** with staff—awareness grows when people see progress.

Start with the Phase 0 list this week; most tasks fit into normal operating hours and cost little or nothing. As revenue grows, reinvest a fixed percentage (many SMEs target 3-5% of IT spend) into the next phases.

You'll wind up with layered defenses aligned to respected frameworks, satisfy marketplace/payment-brand requirements, and—most importantly—sleep better knowing a single phishing email or rogue plugin is vastly less likely to ruin the business you've built.

Here's what Claude 3.7 Sonnet reasoning model recommends:

ESSENTIAL CYBERSECURITY STARTER PLAN (MINIMAL COST)

Here's a streamlined plan focusing on high-impact, low-cost security measures:

Start Here (First 60 Days)

- 1. Enable multi-factor authentication (MFA).** Turn on MFA for all business accounts (email, marketplace accounts, banking). This single step prevents most account takeovers. Cost: Free with most business services.
- 2. Use a password manager.** Install a free or low-cost password manager (Bitwarden has a free tier) Create unique, strong passwords for all accounts. Share passwords securely with team members. Cost: Free to \$3/user/month.
- 3. Back up your critical data.** Identify what data you can't afford to lose. Set up automated backups to cloud storage. Test restoring from backup at least once. Cost: Free to \$10/month depending on data volume.
- 4. Basic security awareness.** Show team members examples of phishing emails. Establish a simple rule: verify unusual requests by phone. Create a "see something, say something" culture. Cost: Free (time investment only).
- 5. Update everything.** Enable automatic updates where possible. Set a monthly reminder to update systems manually. Close unused accounts and services. Cost: Free (time investment only).
- 6. Secure your website.** Enable HTTPS (free certificates from Let's Encrypt). Remove unnecessary plugins and add-ons. Keep e-commerce platform and plugins updated. Cost: Free.

7. **Implement basic fraud checks.** Document what your team already looks for in suspicious orders. Create a simple checklist for verifying orders. Consider address verification for credit card transactions. Cost: Free to implement, may save money by reducing fraud.
8. **Create simple security guidelines.** One-page document of security do's and don'ts. Simple steps for responding to security incidents. List of who to contact if something goes wrong. Cost: Free (time investment only).

Key Threats to Focus On

1. **Phishing attacks** targeting your business accounts
2. **Payment fraud** and suspicious orders
3. **Weak or reused passwords** across business accounts
4. **Outdated software** with known security vulnerabilities

Remember that even with limited resources, these fundamental steps will significantly reduce your risk. Focus on implementing these basics well rather than trying to address everything at once.

AI OVERALL PERFORMANCE

Pretty impressive, 3 different models, all asked the same question, and all performed very well, giving solid recommendations that are low cost and easy to implement! Below are 5 guiding principles to protecting revenue, customer trust, and sleep.

GUIDING PRINCIPLES FOR LEADERS

1. **Prioritize Impact over Exhaustiveness** – A short list done well protects against the attacks small businesses actually face.
2. **Automate the Boring Stuff** – Auto-updates, cloud backups, and fraud-rule engines give 24/7 coverage without headcount.
3. **Make People Part of the Control Stack** – Regular, bite-size training and clear escalation paths are cheaper than tech layers you never configure.
4. **Measure What You Fix** – Simple metrics keep momentum and provide evidence to investors, insurers, and customers.

5. **Plan for “When,” Not “If.”** – A rehearsed one-page response guide turns chaos into an orderly process that limits downtime and reputational damage.

CONCLUSION AND EXECUTIVE ACTION ITEMS

The 2025 cyber-fraud landscape requires proactive, multi-layered defenses. Key actions include:

- **TAKEAWAY #1 TAKE ACTION:** Keep it simple, do the quick wins, use the AI-powered no cost recommendations, take a simple risk assessment (Check out our free-versions on our website), and make a commitment to make progress.
- **TAKEAWAY #2 INVEST IN TRAINING:** Reduce human error through regular education.
- **TAKEAWAY #3 ENHANCE CLOUD SECURITY:** Adopt zero-trust, implement MFA to secure user access and monitor your infrastructure and applications.
- **TAKEAWAY #4 PREPARE RESPONSE PLANS:** Conduct exercises and secure expert support.

Act now to build resilience against evolving threats.

ABOUT FIR RISK ADVISORY

At FIR Risk Advisory, we empower businesses to outsmart fraud through proactive, tailored cybersecurity solutions. Our mission is to deliver **cybersecurity intelligence** and actionable insights that save businesses time on research and prevent attacks before they occur. We specialize in safeguarding organizations against evolving threats, allowing you to focus on growth with confidence.

OUR SERVICES:

- **Fraud Prevention Planning:** Tailored strategies to mitigate fraud risks specific to your business.
- **Cyber Risk Assessments:** In-depth evaluations to identify and address vulnerabilities.
- **Fraud Intelligence Reporting:** Metric driven reporting on emerging fraud threats.
- **Compliance Management:** Expert guidance to ensure regulatory compliance and avoid penalties.

OUR EXPERTISE:

Our team combines extensive experience in **risk management, cybersecurity, financial reporting, audit, technology, and compliance**. We collaborate with best-in-class partners to deliver cutting-edge services, including:

- IT Audit, Cybersecurity, and Data Analytics (Fastrics)
- Penetration Testing and Red Team Exercises (Raxis)
- Security Operations Center (SOC) and Incident Response (Pondurance)
- Digital Transformation and AI Technologies (Altum Strategy Group)

Committed to collaboration, innovation, and client success, FIR Risk Advisory is your trusted partner in navigating the complex cyber-fraud landscape. Visit **FIR Risk Advisory** to learn how we can protect your business today.

RESOURCES

Our 2024 report included the following 12 INSIGHTS and 4 TAKEAWAYS/ACTION ITEMS, which remain very relevant in today's evolving threat landscape, we provide these below as reminder of what we uncovered in last years report:

INSIGHT #1: CYBER CRIME IS BIG BUSINESS AND CONTINUES TO RISE; ALL ORGANIZATIONS ARE AT RISK.

INSIGHT #2: AI IS A GAME CHANGER AND YOU MUST PREPARE NOW!

INSIGHT #3: EMAIL COMPROMISE LEADS TO BIG FRAUD SUCCESS; PATCH EMAIL SERVERS TIMELY AND PROTECT AGAINST SOCIAL ENGINEERING ATTACKS.

INSIGHT #4: BORN-BAD AKA FAKE ACCOUNTS ARE A FOOTHOLD FOR FRAUDSTERS INTO YOUR BUSINESS.

INSIGHT #5: ACCOUNT TAKEOVERS ARE IDEAL FOR FRAUDSTERS TO MASK/HIDE THEIR ACTIVITY WITHIN YOUR REAL CUSTOMERS AND USER ACCOUNTS.

INSIGHT #6: PAYMENT FRAUD IS ONE OF THE EASIEST FRAUDS TO CONDUCT AND RESULT IN CHARGEBACKS AS STOLEN CARD DATA IS USED.

INSIGHT #7: CARD TESTING IS A “FREE SERVICE” TO FRAUDSTERS IF YOUR PAYMENT PLATFORM DOESN’T BLOCK FAKE CARD VERIFICATIONS AND AUTHORIZATIONS.

INSIGHT #8: CRYPTOCURRENCY IS A FOCUS OF THREAT ACTORS.

INSIGHT #9: CLEAN UP OLD SERVICE ACCOUNTS; DISABLE DORMANT USER ACCOUNTS.

INSIGHT #10: EVALUATE YOUR AUTHENTICATION TOKENS/COOKIE ACTIVITY TO VERIFY THE ACCOUNT OWNER IS THE USER ACCESSING THEIR ACCOUNT.

INSIGHT #11: ONE-TIME-PASSWORDS AND PASSCODES CAN BE BYPASSED BY SKILLFUL THREAT ACTORS; USER ACCOUNT HYGIENE IS THE RESPONSIBILITY OF THE ACCOUNT OWNER, BUT ORGANIZATIONS NEED TO ENSURE BEST PRACTICES ARE FOLLOWED.

INSIGHT #12: CHINA AND RUSSIAN STATE SPONSORED THREAT ACTORS ARE AGGRESSIVELY PURSUING UNITED STATES TARGETS & ORGANIZATIONS.

TAKEAWAY #1 ANALYZE YOUR DATA: Financial motives is driving fraudulent activity, all organizations are targets of criminal and state-sponsored threat actors, organizations that do business online are easy targets for abuse, both as a platform for fraud AND as a source of cash and assets for fraudsters. You need to analyze your incoming traffic and transactional data to find the suspicious patterns of activity, deep analysis will reveal the fake/ fraudulent activity. Look and you will find!

TAKEAWAY #2 MANAGE USER ACCOUNTS: Fraudsters will create fake accounts to gain a foothold into your business, they will work hard to crack passwords to takeover user accounts, they will buy stolen credentials and authentication cookies to gain access to your user accounts. Be aware and prepare by analyzing your account usage, define and disable dormant users, identify and disable abusive and fake users, and of course, remove unused service accounts to reduce your attack surface!

TAKEAWAY #3 ENFORCE ACCESS CONTROLS: Help your users maintain secure accounts by enforcing best practices and features for account hygiene; use activity notifications to keep account owners aware of activity; enforce strong password practices; allow users to opt into MFA (or require) to better secure accounts; bind authentication cookies to user fingerprints to ensure the account owner who logged into the account, is the user returning to their account!

TAKEAWAY #4 SECURE WEB APPLICATIONS: Web application attacks is a top risk vector in both breaches and incidents. Identifying and remediating web application vulnerabilities is necessary to better secure your applications and practicing secure coding and software development best practices is key to building security into software designs and driving long lasting improvements.

We rely on open-source information provided by government sponsored organizations and agencies as trusted sources, the below represents a partial listing of those agencies or departments that share quality intelligence.

Cybersecurity and Infrastructure Security Agency (CISA): Established in 2018 within the Department of Homeland Security (DHS), CISA is the national hub for cybersecurity coordination. They provide resources, tools, and guidance to businesses, government agencies, and individuals to strengthen their cybersecurity posture.

Federal Bureau of Investigation (FBI): The FBI investigates cybercrime activities, including hacking, data breaches, and online fraud. They also work to disrupt cyberattacks and bring cybercriminals to justice.

European Union Agency for Cybersecurity (ENISA): ENISA is an agency of the European Union (EU) focused on achieving a high common level of cybersecurity across the member states. They provide advice and expertise to EU institutions and member states, develop cybersecurity tools and methods, and help to raise awareness of cybersecurity risks.

Australia's Australian Cyber Security Centre (ACSC): Part of the Australian Signals Directorate (ASD), the ACSC provides cybersecurity advice and assistance to Australian businesses and individuals. They also work with international partners to combat cybercrime.

Canada's Canadian Centre for Cyber Security (CCCS): The CCCS is a government agency that leads Canada's national effort to combat cyber threats. They offer a variety of resources and services to help businesses and individuals stay safe online.

The United Kingdom's National Cyber Security Centre (NCSC): A part of GCHQ, the NCSC leads the UK government's response to cyber threats. They provide advice and guidance to businesses, government, and the public on how to protect themselves from cyberattacks.

Singapore's Cyber Security Agency (CSA): The CSA is the lead agency for cybersecurity in Singapore. They develop and implement national cybersecurity strategies, oversee incident response activities, and promote cybersecurity awareness.

Interpol: Is the world's largest international police organization. Founded in 1923, it acts as a network connecting law enforcement agencies from 196 member countries.

We also review and source from various authoritative for-profit entities, who provide products and services to help secure business. Those vendors mentioned within this report include:

Verizon DBIR: The Verizon Data Breach Investigations Report (DBIR) is a highly respected annual publication produced by Verizon. It's a valuable resource for anyone interested in understanding cybersecurity threats and trends. We used the 2025 Verizon DBIR extensively in this report, you can find the most recent DBIR and previous editions: verizon.com/dbir/

CrowdStrike: CrowdStrike is a prominent American cybersecurity company headquartered in Austin, Texas, specializing in Cloud Workload & Endpoint Security; Threat Intelligence; and Cyberattack Response Services. The CrowdStrike 2025 Global Threat Report is an excellent resource, download a copy at crowdstrike.com/en-us.

Mandiant (Google Cloud Security): Founded in 2004 by Kevin Mandia, Mandiant earned its reputation by parachuting into some of the most high-profile breaches on record and distilling that frontline experience into the annual M-Trends report. The team now combines Google's planet-scale telemetry with its own 450,000-plus hours of investigation work each year to deliver managed detection & response, incident-response retainer services, and threat research. Download 2025 M-Trends [here](#).

Palo Alto Networks Unit 42: Unit 42 is the threat-intelligence and incident-response arm of Palo Alto Networks, created in 2014 and today led by Senior VP Sam Rubin. In its latest Global Incident Response Report the team responded to more than 500 engagements in 2024. Download 2025 Global Incident Response Report [here](#).

IBM Security X-Force: X-Force is IBM's global cadre of "hackers, responders, researchers and analysts," active in 170 countries and monitoring some 150 billion security events every day. Its annual Threat Intelligence Index (now in its 12th edition) distills those observations. Download your copy [here](#).

Resources to help you evaluate your security posture and advise on best practices to protect your business (all the Government sponsored sites listed above also provide security guidance and best practices):

National Institute of Standards and Technology (NIST): NIST develops cybersecurity frameworks and standards that businesses and government agencies can use to improve their cybersecurity posture. They also conduct research on cybersecurity technologies and best practices. <https://www.nist.gov/>

The Center for Internet Security (CIS): CIS is a non-profit organization founded in 2000 that works to improve cybersecurity for everyone. They develop and share best practices to help individuals, businesses, and governments defend against cyber threats. CIS achieves this through CIS Controls and CIS Benchmarks. <https://www.cisecurity.org/>

Open Worldwide Application Security Project (OWASP): OWASP is a non-profit organization that acts as a global community for web security. They provide free resources like articles, tools, and documentation to improve software security, with a focus on web applications and Internet of Things (IoT) devices. Their most well-known project is the OWASP Top 10, which is a regularly updated list of the most critical web application security risks. <https://owasp.org/>