Data Defense: Creating a Robust Fraud Awareness Plan to Protect Your Company

Welcome to the world of cyber theft. Today's hackers are savvy businesspeople, making cybercrime their full-time job. They find new ways to attack your systems, sometimes waiting months to strike. Cybersecurity is a business issue, and prevention costs far less than recovering from fraud.

Every Business Needs a Fraud Awareness Plan

Planning ahead requires multiple levels of mitigation. At home, layered protection, such as bolt lock, chain, and alarm system, deters burglars. The same applies to your business: the more layers of mitigation you have, the more likely cybercriminals will look elsewhere.

2023 saw a 22% YOY increase in losses suffered due to cybercrime.[1]

Form a Fraud Awareness Advisory Council of Key Players

A team a trusted advisors can provide the confidence, support, and know-how for your company's long-term success. It may include such key players as:

Information Technology- to defend against current threats and anticipate future risks. Your team should:

Implement a Multilayered Security Infrastructure

- Deploy advanced firewalls with Intrusion Detection Systems (IDS) to monitor and filter traffic. Use next-gen firewalls with deep packet inspection and behavioral analysis to prevent sophisticated threats.
- Utilize Endpoint Detection and Response (EDR) solutions for real-time visibility and rapid response to endpoint threats on all devices.
- Isolate network segments to limit malware spread and unauthorized access, reducing the attack surface and containing breaches.

Secure Data Storage and Transmission

To ensure secure data storage and transmission, implement AES256 or equivalent encryption for data at rest and in transit, both in data centers and during network transmission. Additionally, deploy SSL/TLS certificates to secure websites and applications, ensuring encrypted connections and protecting against data interception.

Implement Rigorous Access Controls

Enforce Multifactor Authentication (MFA) for all users to require multiple verification methods, reducing the risk of unauthorized access even if credentials are compromised.

Accounting- to review role-based access controls to ensure employees have the minimum level of access required for their roles. Regularly update access permissions to reflect changes in roles and responsibilities.

Insurance- to provide liability coverage for a breach — not to mention business interruption costs and recovery fees.

Legal- to make sure you report the attack according to disclosure laws.

continue >

Public Relations- to be ready with an action plan to manage the blow to your business's reputation.

Finance- to know your plan and how it can dovetail with the fraud protection services used by your company. You'll want to ensure that your bank offers a positive pay service. It enables the bank to compare the checks or ACH transactions you originate against the data in its system. Most banks offer a form of check and ACH Positive Pay services.

Build a Robust Backup Plan to Fortify Your Defense

Smart planning protects you from emerging threats. Here are three security strategies to put in place with your IT team:

1. Automated Backups

Schedule secure, off-site backups of critical data. Use both cloud and physical backups to prevent data loss, ensuring that they are immutable.

2. Disaster Recovery

Develop and regularly update a disaster recovery plan to restore systems and data after breaches or disasters. Regularly test its effectiveness.

3. Incident Response Procedures

Create detailed procedures for identifying, containing, eradicating, and recovering from fraud incidents.

Take Charge of Cybersecurity: Planning, Training, Testing, and Response

A successful Fraud Awareness Plan involves regular employee training, refresher courses, and drills. Stay informed and adapt to emerging threats by subscribing to threat intelligence services that provide insights into new vulnerabilities in your industry, allowing proactive adjustments to your security strategies.

Regularly conduct vulnerability assessments with tools like Nessus or OpenVAS to identify and address security weaknesses in your systems. Additionally, engage professional penetration testers to simulate real-world attacks, uncover vulnerabilities, and use the findings to bolster your security posture.

Remember, a practiced incident response plan is essential for swift recovery from breaches. Cybersecurity is your responsibility, and while breaches can have significant fallout, trained staff and robust resources will help secure your business now and into the future.

Want more information on protecting your company from cyber threats?
Connect with Webster Bank.

[1]FBI Internet Crime Report 2023

COM-WP 09/24