THE NATIONAL CYBERSECURITY SOCIETY

Business Identity Theft in the U.S.

Report Summary Presented to CERCA

May 16, 2018

Agenda

- Background
- Study Purpose
- What is it?
- Identity Management Challenges
- Business Credit File/CRAs
- Victim Resources
- Vulnerabilities/Gaps
- Recommendations

Background

- NCSS awarded federal grant (NITVAN) to lead a national coalition
- NITVAN is a network of coalitions engaged in creating, enhancing and delivering identity theft and identity theft related crime victim assistance training and outreach
- Focus on threats from cyberspace
- Training, awareness, technical assistance and policy guidance to victims

- ***FUNDS derived from fines and penalties paid by convicted federal offenders***

Purpose

- Conduct a study to lay the foundation of a national program
- Evaluate the statutes, ecosystem - federal/state/private sector
- Evaluate the crime from an IT security perspective
- Identify gaps and vulnerabilities exploited
- Identify victim resources/identify coalition partners
- Initiate a national discussion with coalition partners

Business Identity Theft defined:

- FTC defines identity theft:
  - “as a fraud that is committed or attempted using a person’s identifying information without authority”
- DoJ Office for Victims of Crime defines business identity theft:
  - “as a type of identity theft committed with the intent to defraud or hurt a business, (e.g. financial business identity, extortion)”
- IRS defines business identity theft:
  - “as creating, using or attempting to use a businesses’ identifying information without authority to obtain tax benefits”

Types of business identity theft:

Using a business's identity, four theft types emerged from research:

1. **FINANCIAL FRAUD** – obtaining new lines of credit, loans or credit cards, UCC fraudulent filings
2. **TAX FRAUD** – filing fraudulent returns using tax credits/subsidies to obtain both federal and state refunds
3. **WEBSITE DEFACEMENT** – manipulating a business's identity on the web
4. **TRADEMARK RANSOM** – registering a business name as an official trademark and demanding a ransom for release of the trademarked business name
5. SIMILAR – ***Business email compromise***

How bad is it?

IRS:

  - *“Small business identity theft is big business for identity thieves”*
  - In the past year (2017) 250% increase in the number of fraudulent returns to include filings for partnerships, estates and trusts.

- D&B:
  - Significant increase in business identity theft for the 6 year period 2012-2018
  - Largest number of business identity theft – LA, Las Vegas, Miami, Atlanta, Houston and New York
- IC3
  - 270% increase in identified victims, with total exposed losses at $1.2 B

Identity Management Challenges:

- Business Identity Data is public, non-sensitive data
- Readily available on the Internet – state business records, D&B, EIN look ups, DNS records, online search engines
- Easy to change state records without challenge
- Federal uses EINs, States use DBA
- Only one state offers two factor authentication
- Only 1 state (California) verifies name availability
- Limited adoption of alert notifications when state records are changed

Business Credit File

- Good credit probably one of the most coveted assets a business has, yet rarely do businesses implement protections
- Statues cover consumers, not businesses
- Difficult to monitor credit unless businesses sign up for credit monitoring services
- All use different data to assess credit – data not readily available except for D&B
- CRAs rely on state records; D&B will respond and investigate potential fraud when notified by business
- Advice to businesses is inconsistent and often not valid
- No Fraud Alerts/Freeze File processes for businesses

Victim Resources

- IRS 14039-B Business Identity Theft Affidavit
- IRS – Tax Practitioner Guide to Business identity Theft
- D&B investigation support
- State Business Registry Offices
- Identity Theft Resource Center (ITRC)
- NCSS

Vulnerabilities/Gaps

- EINs and SSNs
- Compromised Websites
- Federal Resources – lack of statistics
- Limited to no Cross State Coordination
- Limited public awareness
- State Registration Systems
- Identity Verification
- Data Validity/Accuracy/Data Availability/Access
- Limited Understanding of Business Credit File Restitution processes

Recommendations

- National Business Identity Task Force
- Business Identity Guidebook
- Increase Public Awareness
- State Registration Systems
- Credit Reporting Agencies
- Statutes
- Federal Agency/Law Enforcement
- Improve Victim Resources

How to contact us:

The National Cybersecurity Society
1215 31st Street, NW #3921
Washington, DC 20027

Contacts:
Mary Ellen Seale – ME@theNCSS.org
Chiranjeev Bordoloi – CJ@theNCSS.org

Or visit our website:
www.nationalcybersecuritysociety.org

Follow us on Twitter:
@TheNCSS