IRS Nationwide Tax Forum 2019

Data Compromise Playbook for Tax Practitioners

SA Carlos L. Ramón

Internal Revenue Service

Criminal Investigation

CI Mission

- Investigate criminal violations of the IRC and related financial crimes
- Foster confidence in the tax system and law compliance

Why a tax professional need a cyber security plan?

https://www.youtube.com/watch?v=IEZrN2ThoB4

IRS Tax Forum | IRS Nationwide | 2019

Background

- NIST Cybersecurity Framework
- IRS Publication 4557- Safeguarding Taxpayer Data
- It’s the law- FTC- Safeguard Rule

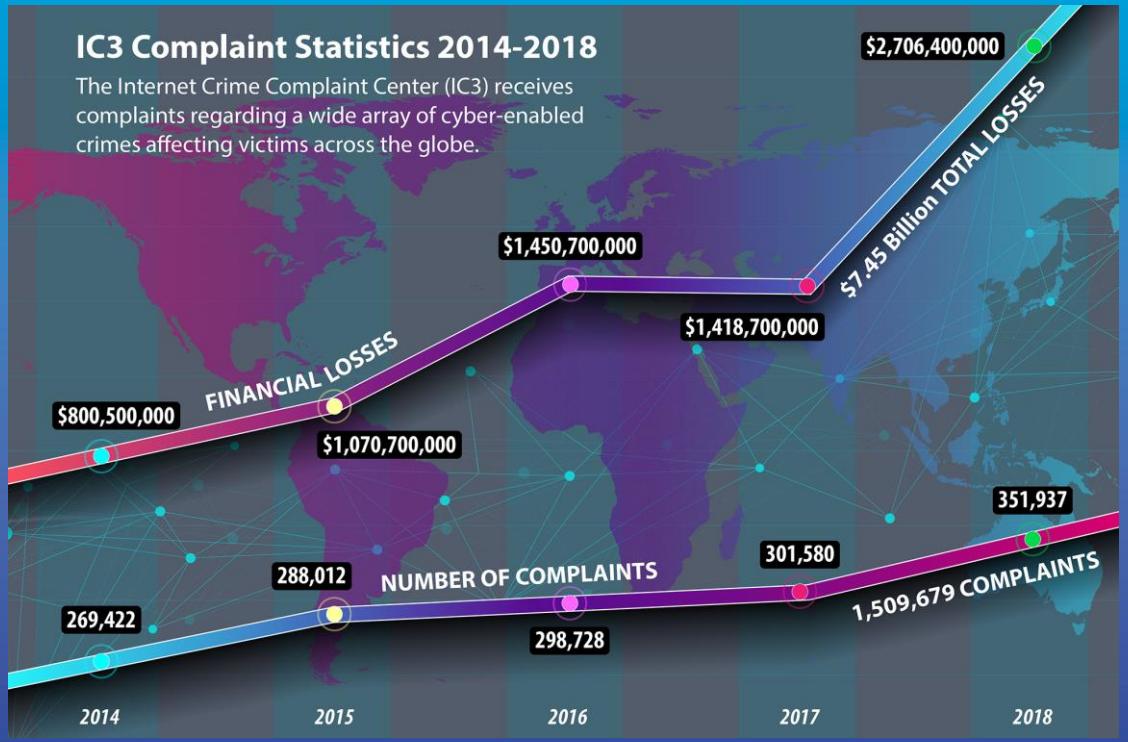
Safeguarding Client Data

Federal Laws Apply to Preparers:

- Gramm-Leach-Bliley Act, the “Safeguards Rule” requires you to ensure the security and confidentiality of customer records and information.
- Gramm-Leach-Bliley Act, the “Financial Privacy Rule” deals with privacy notices and information collection and sharing.
- Internal Revenue Code (IRC) imposed criminal and monetary penalties for knowingly or recklessly making unauthorized disclosures.

IRS Tax Forum | 2019 IRS Nationwide

What is the Problem?



Source: FBI 2018 Internet Crime Report- IC3

Problem

- Business Email Compromises- BEC
  2018- 20,373 Complaints
  $1.2 billion in adjusted losses

- IRS- 118 incidents with over 88,374 TINs and over $17M in revenue protected.

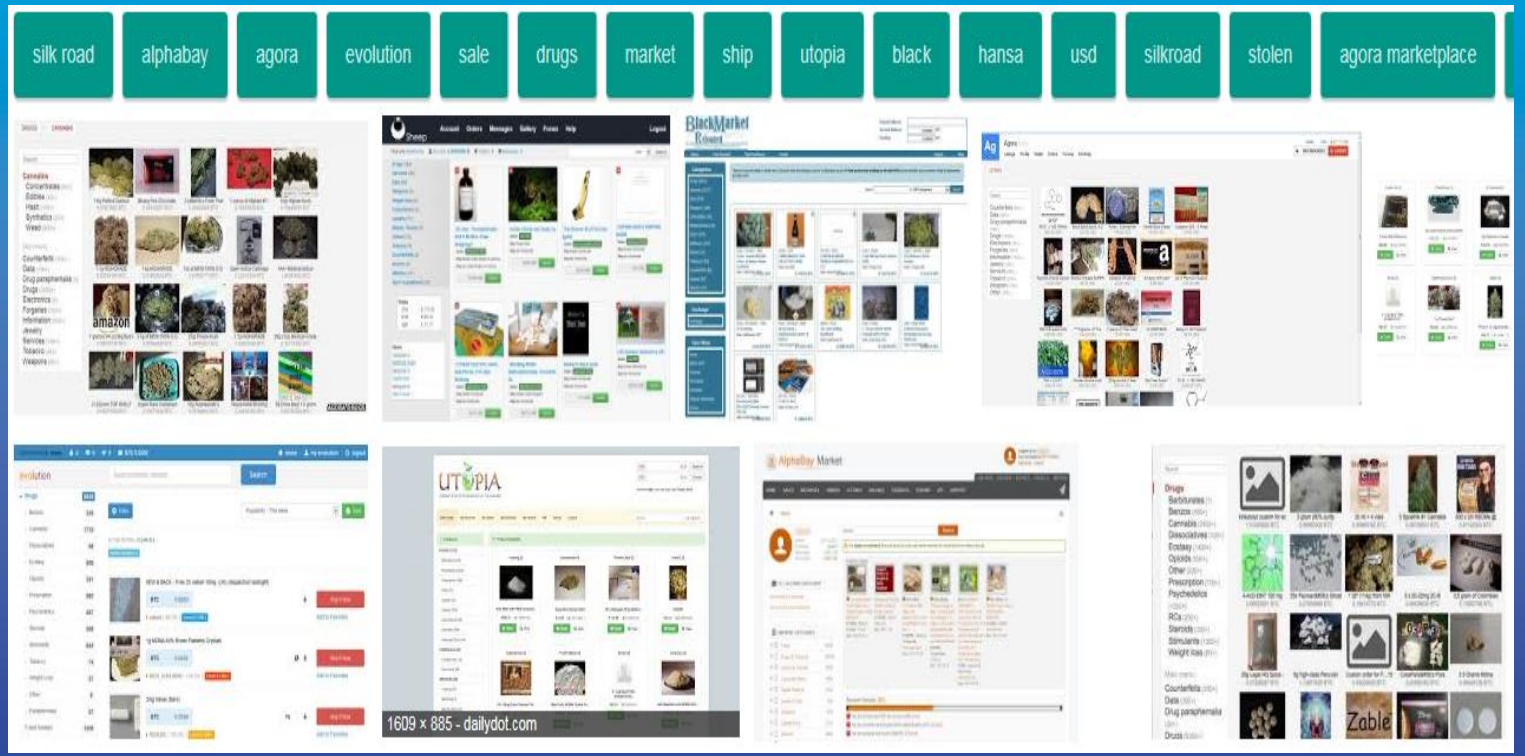
Source: 2018 Internet Crime Report- IC3 and DSL TIN Report

Problem


THIS DOMAIN HAS BEEN SEIZED
The domain for
xDedic
has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant
issued by the United States District Court for the Middle District of Florida
under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:
DEPARTMENT OF JUSTICE
CRIMINAL INVESTIGATION
DEPARTMENT OF THE TREASURY
SPECIAL AGENT
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FCCU
Federal Police
federal prosecutor's office
HOMELAND SECURITY INVESTIGATIONS
SPECIAL AGENT
National High Tech Crime Unit
BUNDESKRIMINALAMT
CYBER INTELLIGENCE OPERATIONS
EUROPOL
CYBERPOLICE DEPARTMENT
NATIONAL POLICE OF UKRAINE

What is the Dark Web?

Examples of the Markets



NIST Cybersecurity Framework

Five key pillars of the successful and holistic cybersecurity program

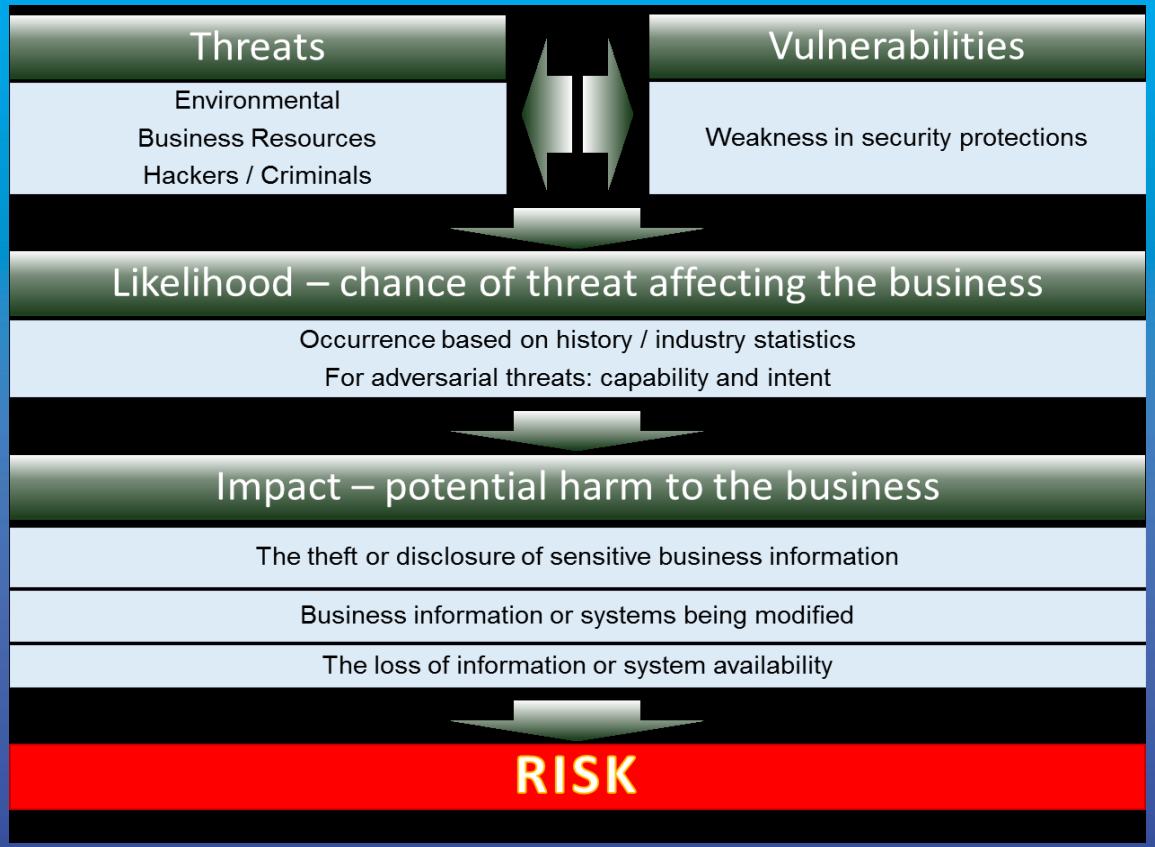
Source: www.nist.gov/cyberframework

Tax Preparer guide

- Identify physical and software assets
- Identify cybersecurity policy

Source: IRS Pub 4557; www.nist.gov/cyberframework

IRS Tax Forum | 2019 IRS Nationwide



Source: NIST-Small Business Information Security: The fundamentals

The Protect Function

- Establish a Data security protection plan – CIA
- Manage Protective Technology
- Equipment

Source: IRS Pub 4557; www.nist.gov/cyberframework

CIA

- **Confidentiality** - protecting information from unauthorized access and disclosure.
- **Integrity** - protecting information from unauthorized modification.
- **Availability** - preventing disruption in how you access information.

Source: NIST-Small Business Information Security: The fundamentals

Cybersecurity

- **Physical Security** – e.g. using fences and locks;
- **Personnel Security** – e.g. using background checks;

- **Contingency Planning and Disaster Recovery** – how to resume normal operations after an incident, also known as Business Continuity Planning;
- **Operational Security** – protecting business plans and processes, and
- **Privacy** – protecting personal information.

Source: NIST-Small Business Information Security: The fundamentals; IRS Pub 4557

Review internal controls

- Install anti-malware/anti-virus security software
- Use strong passwords, protect wireless devices
- Encrypt all sensitive files/emails
- Back up sensitive data to a safe (external source)
- Wipe clean or destroy old equipment
- Limit access to taxpayer data (need to know)

Source: IRS Pub 4557- Safeguarding taxpayer data

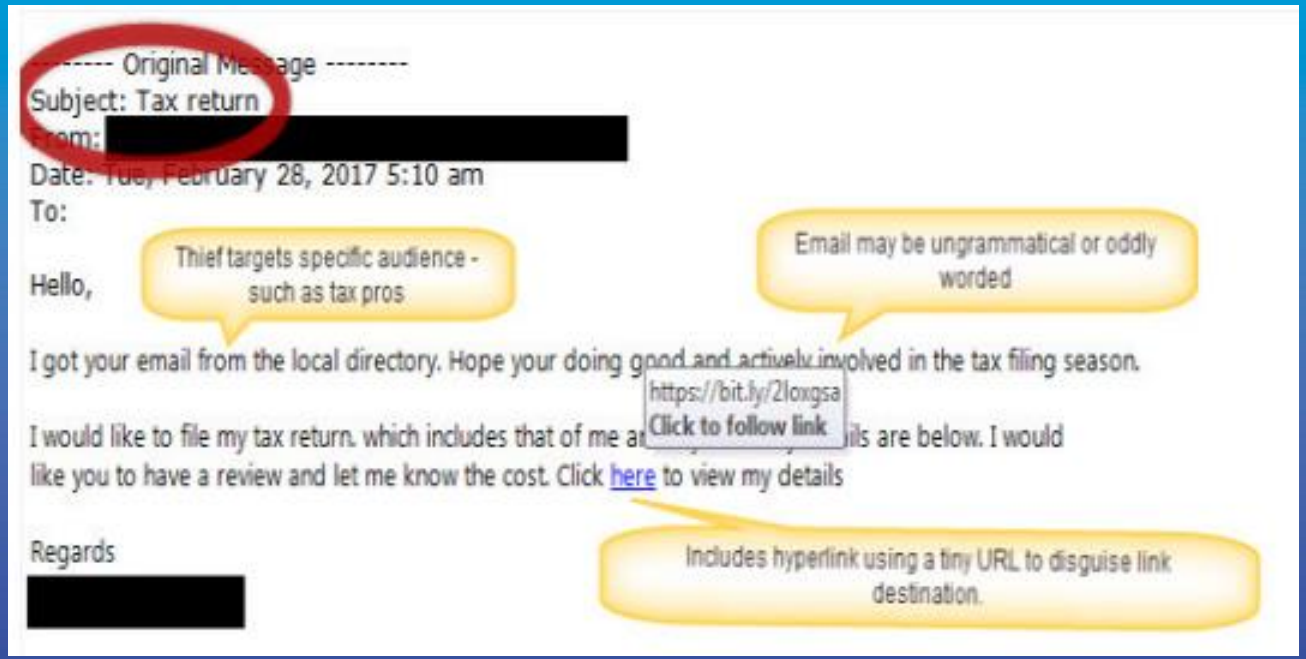
IRS Tax Forum | IRS Nationwide | 2019

The Detect Function

- Implementing security continuous monitoring capabilities to monitor cybersecurity events
- Ensuring anomalies and events are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures

Source: IRS Pub 4557; www.nist.gov/cyberframework

Recognize a Phishing Scam



Ransomware

- Usually comes in the form of Phishing email and has attachments or links.
- Ransomware is a type of malware that restricts access to infected computers and requires victims to pay a ransom to regain access to their data
- Typical ransoms are in the range of $100 - $300, and are often demanded in the form of digital currency, such as Bitcoin

Ransomware

Business Email Compromise

- Cybercriminals are able to **identify** chief operating officers, school executives or others in position of authority (Social Engineering).
- Fraudsters mask themselves as executives or people in authoritative positions and send emails to payroll or human resources requesting copies of Forms W-2. **(Grooming)**
- Form W-2 contains the following **(Exchange of Information)**

  Employment Identification Numbers (EIN)
  Social Security Numbers
  Income / Withholdings (Federal, State, Local)
  Address
  Retirement Plan
  Health Benefits Plan

Business Email Compromise

-----Original Message-----
From: Mickey Mouse <mk@mu.se>
Sent: Tuesday, January 22, 2019 1:03 PM
To: Minnie Mouse <minnie@realbusiness.org>
Subject: Request

Hi Minnie,

I need you to email me 2018 W2s of all employees. How soon can you get me those?

Regards
Mickey Mouse

Example: Warning Labels

From: [redacted] [mailto:[redacted]]
Sent: Tuesday, June 12, 2018 2:01 AM
To: [redacted]. <[redacted]>
Subject: Final Reminder for Notice of Tax Overpayment

**** This is an EXTERNAL email. Exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email. ****

1

Signs of a Breach- The Victim Experience

- **Electronic Return Rejected (Paper Return)**
- **Verification Letters (**5071C or 4883C)
- **https://www.irs.gov/individuals/irs-notice-or-letter-for-individual-filers** External
- **Transcripts**
- **Receipt of US Treasury Refund Check**
- **Receipt of Reloadable Prepaid Card**
- **Receipt of Refund Transfer Company Check**

Respond

- Ensuring Response Planning processes are executed during and after an incident
- Managing Communications during and after an event
- Analyzing effectiveness of response activities

Source: IRS Pub 4557; www.nist.gov/cyberframework

What to do after a tax professional data compromise

https://www.youtube.com/watch?v=9OPqsuG-jVQ

Source: IRS Pub 4557; www.nist.gov/cyberframework

Respond

- Contact IRS Stakeholder Liaison When Compromise Detected
  - Stakeholder Liaison will refer Information within IRS (i.e. Criminal Investigations, Return Integrity & Compliance Services)

- Follow State Reporting Requirements (i.e. State Attorney General, State Consumer Protection Bureaus, State Police)

- Report Compromise to FBI, US Secret Service, Federal Trade Commission

Source: IRS Pub 4557; www.nist.gov/cyberframework

Respond

- Contact experts:
  - Security expert – to determine the cause and scope of the breach, to stop the breach and to prevent further breaches from occurring.
  - Insurance company – to report the breach and to check if your insurance policy covers data breach mitigation expenses.

Source: IRS Pub 4557; www.nist.gov/cyberframework

IRS Security Summit

- The Security Summit has launched a campaign aimed at increasing awareness among tax professionals: Protect Your Clients; Protect Yourself. This is a follow-up effort to the “Taxes. Security. Together.” public awareness campaign

IRS Tax Forum | IRS Nationwide | 2019

Recover

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities

Source: IRS Pub 4557; www.nist.gov/cyberframework

Recover

- Update your IRS Stakeholder Liaison with developments;
- Review FTC's Data Breach Response: A Guide for Business
- Determine how the intrusion or theft occurred Develop a continuity plan.
- Make full backups of all business data and files. If you weren't doing it before the data loss, start as soon as your systems are clean.

Source: IRS Pub 4557; www.nist.gov/cyberframework

Recover

- A routine backup means a data loss or ransomware attack (as well as a hurricane or flood) will not destroy all files.
- Encrypt backed up files.
- Consider a monthly backup schedule, or more often during the filing season.
- Backup files after completing a routine system scan.
- Use an external hard drive or cloud storage; encrypt files prior to uploading to the cloud.

Source: IRS Pub 4557; www.nist.gov/cyberframework

NIST Cybersecurity Framework

Five key pillars of the successful and holistic cybersecurity program

Source: www.nist.gov/cyberframework

Use the Safeguard Rule Checklist

ONGOING	DONE	N/A	Employee Management and Training
☐	☐	☐	
☐	☐	☐	

			Information Systems
			Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:
☐	☐	☐	
☐	☐	☐	

			Detecting and Managing System Failures
			Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:
☐	☐	☐	Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses.

Source: IRS Pub 4557

Sources

- **Tax Tips (https://www.irs.gov/uac/irs-security-awareness-tax-tips)**
  - Safeguarding Taxpayer Data: Create Strong Passwords

    Protect Your Clients; Protect Yourself Tax Tip Number 8, January 25, 2017
  - What to Do If You Suffer a Data Breach or Other Security Incident

    Protect Your Clients; Protect Yourself Tax Tip Number 7, January 18, 2016
  - Safeguarding Taxpayer Data: Monitor Your EFIN for Suspicious Activity

    Protect Your Clients; Protect Yourself Tax Tip Number 6, January 11, 2017
- **Publications**
  - Publication 4557, Safeguarding Taxpayer Data
  - Publication 4524, Security Awareness for Taxpayers
- **Related IRS.gov Resources**
  - **Videos, alerts, fact sheets, news releases**

Sources

Federal Trade Commission "Start With Security"

https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Department of Commerce's National Institute of Standards and Technology (NIST)

Small Business Information Security: The Fundamentals

https://www.nist.gov/cyberframework

Center for Internet Security (CIS)

https://www.cisecurity.org/critical-controls.cfm

Questions & Contact Information

Special Agent- Refund and Cyber Crimes
Carlos L. Ramon
(787)-625-6511
Carlos.ramon@ci.irs.gov

IRS Tax Forum IRS Nationwide 2019