



# Data Compromise Playbook for Tax Practitioners





# CI Mission

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





# Background

- **NIST Cybersecurity Framework**
- **IRS Publication 4557- Safeguarding Taxpayer Data ([irs.gov/protectyourclient](https://irs.gov/protectyourclient))**
- **It's the law- FTC- Safeguard Rule**





# Safeguarding Client Data

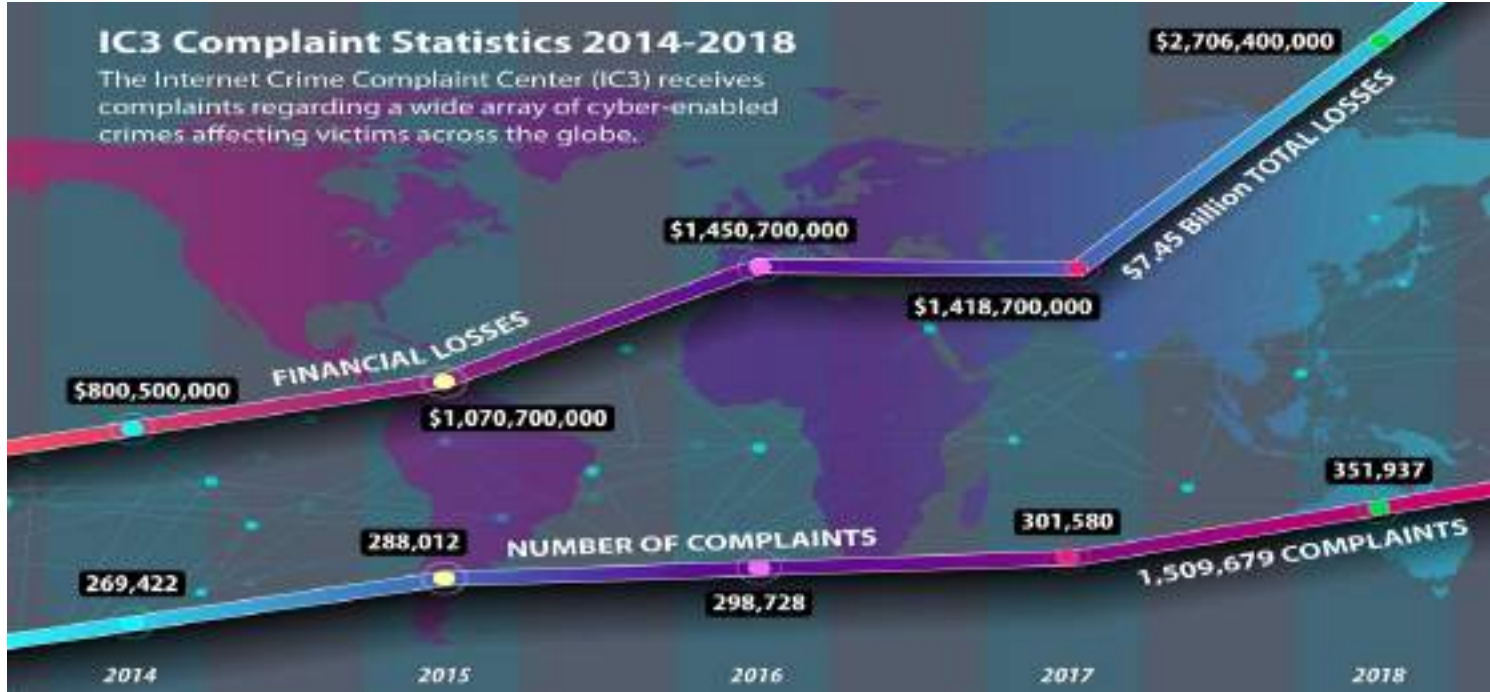
## Federal Laws Apply to Preparers:

- **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.





# What is the Problem?



Source: FBI 2018 Internet Crime Report- IC3



# More of the 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.





# Enhances the Problem

## THIS DOMAIN HAS BEEN SEIZED

The domain for

### xDedic

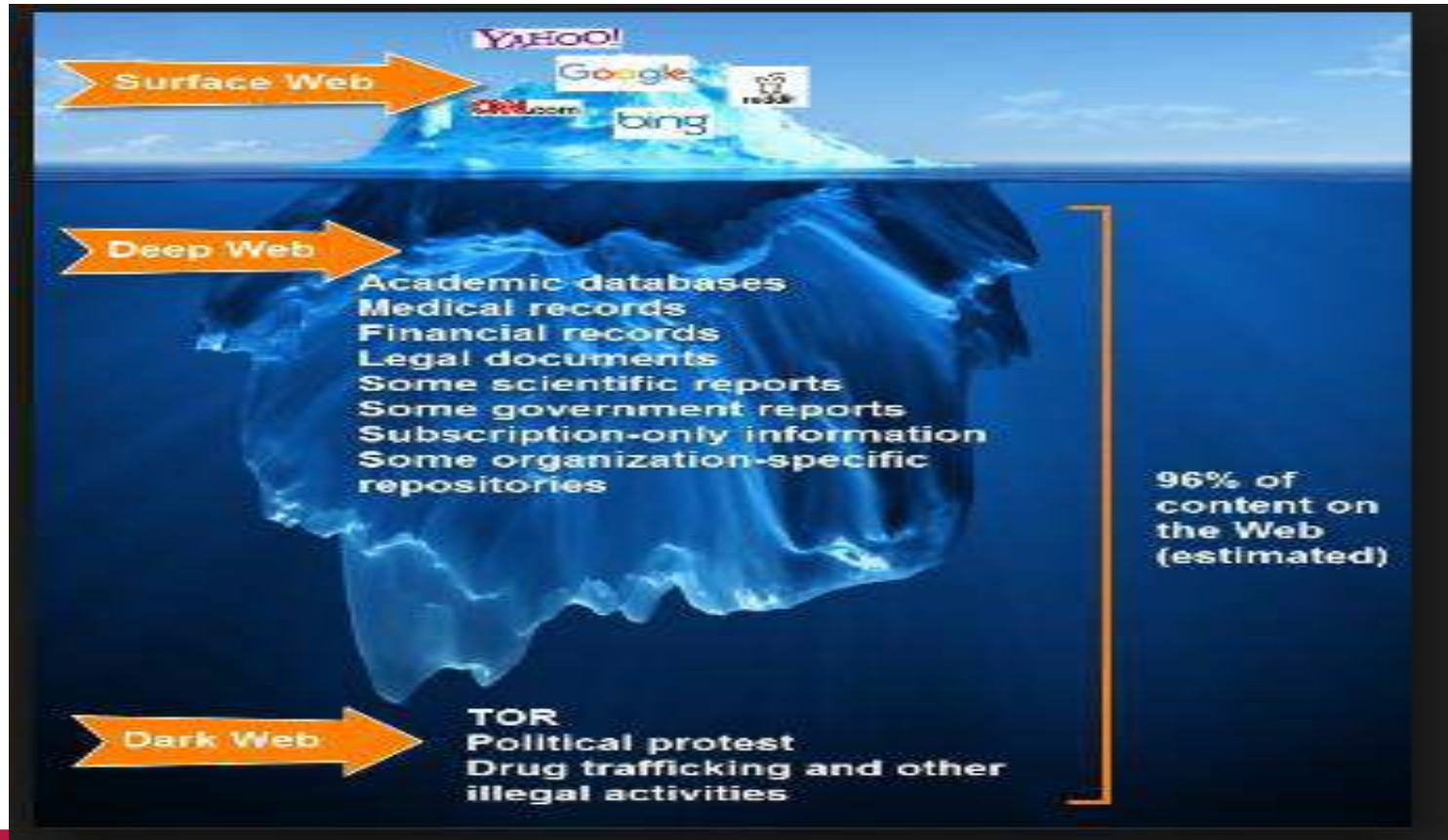
has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Middle District of Florida under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:







# What is the Dark Web?







# Examples of the Markets

- silk road
- alphabay
- agera
- evolution
- sale
- drugs
- market
- ship
- utopia
- black
- hansa
- usd
- silkroad
- stoken
- agora marketplace





# NIST Cybersecurity Framework

Five key pillars of the successful and holistic cybersecurity program



Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



# NIST Cybersecurity Framework

- Identify physical and software assets
- Identify cybersecurity policy





# Risk Management



Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



# The Protect Function

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



**Source:** [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



- **C**onfidentiality - protecting information from unauthorized access and disclosure.
- **I**ntegrity - protecting information from unauthorized modification.
- **A**vailability - preventing disruption in how you access information.







- **Physical Security**
- **Personnel Security**
- **Contingency Planning and Disaster Recovery**
- **Operational Security**
- **Privacy**





# 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:** [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



# 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**





# Recognize a Phishing Scam

----- Original Message -----

Subject: Tax return

From: [Redacted]

Date: Tue, February 28, 2017 5:10 am

To:

Hello,

Thief targets specific audience - such as tax pros.

Email may be ungrammatical or oddly worded

I got your email from the local directory. Hope your doing good and actively involved in the tax filing season.

I would like to file my tax return, which includes that of me and my family. <https://bit.ly/2loxgsa> Click to follow link. Details are below. I would like you to have a review and let me know the cost. Click [here](#) to view my details

Regards

[Redacted]

Includes hyperlink using a tiny URL to disguise link destination.





# 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

Wana Decrypt0r 2.0

**Ooops, your files have been encrypted!**

not so enough time.  
 You can decrypt some of your files for free. Try now by clicking <Decrypt>  
 But if you want to decrypt all your files, you need to pay.  
 You only have 3 days to submit the payment. After that the price will be d  
 Also, if you don't pay in 7 days, you won't be able to recover your files for  
 We will have free events for users who are so poor that they couldn't pay

**How Do I Pay?**  
 Payment is accepted in Bitcoin only. For more information, click <About>  
 Please check the current price of Bitcoin and buy some bitcoins. For more  
 click <How to buy bitcoins>.  
 And send the correct amount to the address specified in this window.  
 After your payment, click <Check Payment>. Best time to check: 9:00am  
 GMT from Monday to Friday.  
 Once the payment is checked, you can start decrypting your files immediat

**Contact**  
 If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable you  
 for a while, until you pay and the payment gets processed. If your anti-virus gets  
 updated and removes this software automatically, it will not be able to recover your  
 files even if you pay!

English  
 English  
 Bulgarian  
 Chinese (simplified)  
 Chinese (traditional)  
 Croatian  
 Czech  
 Danish  
 Dutch  
 Filipino  
 Finnish  
 French  
 German  
 Greek  
 Indonesian  
 Italian  
 Japanese  
 Korean  
 Latvian  
 Norwegian  
 Polish  
 Portuguese  
 Romanian  
 Russian  
 Slovak  
 Spanish  
 Swedish  
 Turkish  
 Vietnamese

**Payment will be raised on**  
 1/4/1970 00:00:00  
 Time Left  
 00:00:00:00

**Your files will be lost on**  
 1/8/1970 00:00:00  
 Time Left  
 00:00:00:00







# 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**





# Business Email Compromise

- **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**



Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



# 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

---



**Source:** [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



# 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



Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



# 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





# Signs of a Breach- The Victim Experience

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







# 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**





# 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.**





# 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.**





# 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





# Recover

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





# 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.**







# 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.





# NIST Cybersecurity Framework

Five key pillars of the successful and holistic cybersecurity program



Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

# Use the Safeguard Rule Checklist

ONGOING	DONE	N/A
---------	------	-----

## Employee Management and Training

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

## Information Systems

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

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:

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

## Detecting and Managing System Failures

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

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:

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses.



Source:  
**IRS**



# 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**



# Sources

## 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>







# ***Multi-Factor Authentication***





# Communications & Liaison STAKEHOLDER LIAISON



## Sign Up

If you don't have an IRS username, go back and create an account.

[← BACK](#)

## Log In

Already have a username? Welcome back!

Username

[LOG IN >](#)

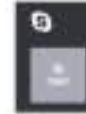
[Forgot Username](#)

*PTIN and FIRE users need a separate account in this system*





# Communications & Liaison STAKEHOLDER LIAISON



## Log In

Verify that your Site Image and Site Phrase below are correct. If the Site Image and Site Phrase are not correct, please do not proceed.

Your Site Image:



Your Site Phrase:

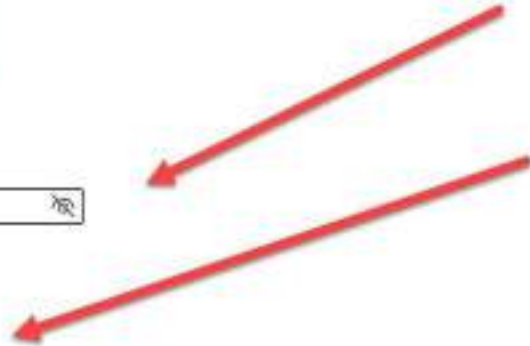
Maggie's Stuff

Password

[Forgot Password](#)

SUBMIT >

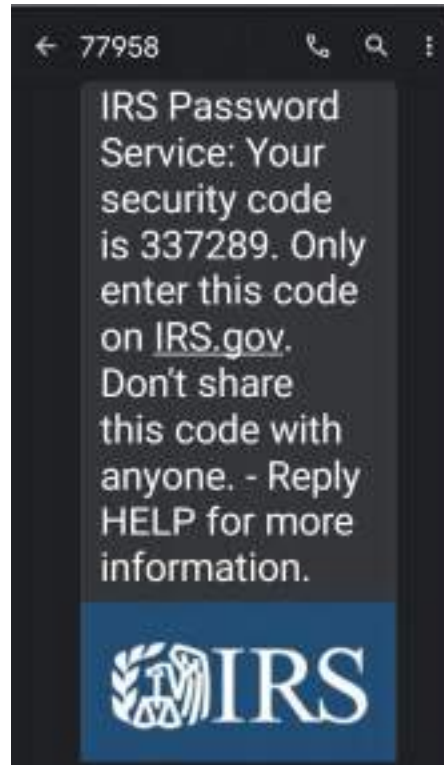
CANCEL





# Communications & Liaison

## STAKEHOLDER LIAISON





# Questions

## Contact Information

**Jill A. Maniacci, M.S. and E.A.**

**1 Kalisa Way, MS #393**

**Paramus, NJ 07652-3516**

**Phone: (201) 986 – 5131**

**E-fax: (877) 877 – 7361**

**[Jill.A.Maniacci@irs.gov](mailto:Jill.A.Maniacci@irs.gov)**

