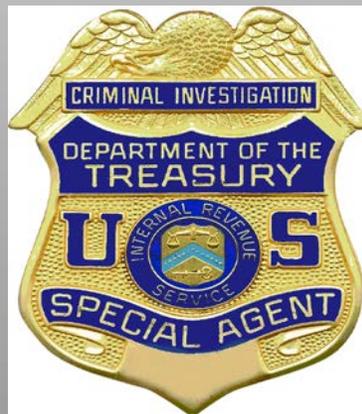


Data Compromises a Tax Practitioners “Nightmare”

Name: Brian Thomas
Title: National ID Theft Coordinator
IRS Criminal Investigation

Internal Revenue Service Criminal Investigation

Criminal Investigation serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.



Overview

- **IRS Publication 4557/NIST “Small Business Information Security: The Fundamentals”**

<https://www.irs.gov/uac/publication-4557-safeguarding-taxpayer-data>

<https://www.irs.gov/pub/irs-pdf/p4557.pdf>

<http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

- **Identify:** Data, People, Equipment “**The Printer Breach**”
 - **Protect:** Limit Access, Updates, Firewalls, “**Lost Passwords and Remote Access Breaches**”
 - **Detect:** Anti-Virus, Spyware, “**Lost Passwords to Spear Phishing and Malware Breaches**”
 - **Respond:** Information Security Plan
 - **Recover:** Backups, “**Ransomware Attack**”
- **Cyber Security Resources**



Identify

- **Identify and control who has access to your business information**
- **Conduct Background Checks**
- **Require individual user accounts for each employee**
- **Create policies and procedures for information security**

Identify

- ***Identify what information your business stores and uses***

	Example: Client files	Payroll Data	Employee Files		
Cost of revelation (Confidentiality)	High				
Cost to verify information (Integrity)	High				
Cost of lost access (Availability)	High.				
Cost of lost work	High				
Fines, penalties, customer notification	High				
Other legal costs	High				
Reputation / public Relations costs	High				
Cost to identify and repair problem	High				
Overall Score:	High				

Identify

- ***Develop an Inventory of IT Related Equipment***

	Description (e.g. nickname, make, model, serial number, service ID, other identifying information)	Location	Type of information the product comes in contact with.	Overall Potential Impact
1	Cell phone; Type – Sonic; Version – 9.0 ID – “Police Box”	Mobile T&S Network	Email; Calendar; Customer Contact Information; Photos; Social Media; Locations; Medical Dictionary Application	High
2	Computers			
3	Printers			
4	Wireless Routers			
5	Remote Access			

Identify

Practitioner Breach 1 “The Printer”

- Office printer with wireless capabilities hooked to network
- Manufacturer default password never changed
- Perpetrator gained access via printer’s wireless capabilities and manufacturer default password
- Gained full access to Firm’s files

Identify

The screenshot shows a Microsoft Edge browser window displaying a news article on the NBC News website. The browser's address bar shows the URL <http://www.nbcnews.com/news/us-news/data-breach-pip-pr>. The page title is "Data Breach at PIP Printing Company Leaks Thousands of Highly Sensitive Documents". The article is dated "FEB 11 2017, 3:08 PM ET" and is written by "MARY EMILY O'HARA". The main text of the article is highlighted in blue, indicating it has been identified. The text includes: "An online security breach at a national printing chain leaked thousands of sensitive documents — from labor filings involving NFL players to lawsuits against Hollywood studios to personal immigration-related papers — raising the possibility that private information could end up in the wrong hands." "The leak at PIP printing, which has more than 400 locations in 13 countries, went on for four months before it was repaired Tuesday, cybersecurity experts involved in investigating the breach told NBC News. But there's no evidence that any hackers may have stumbled upon the files to use them for malicious purposes, they add." "The documents, which NBC News examined, ranges from emails revealing credit card and social security numbers to legal filings such as depositions, subpoenas and labor lawsuits. Extensive medical records belonging to high-profile athletes were also at risk." The browser window also shows a sidebar with "SHARE" options (Share, Tweet, Email, Print) and a "FROM THE WEB" section with sponsored links. The Windows taskbar at the bottom shows the time as 8:39 AM on 06/29/2017.

Protect

- **Limit employee access to data and information**
- **Patch your operating systems and applications**
- **Install and activate software and hardware firewalls on all your business networks**
- **Secure your wireless access point and networks**
- **Set up web and email filters**
- **Use encryption for sensitive business information**
- **Dispose of old computers and media safely**
- **Train your employees**

Protect

Practitioner Breach 2 “Remote Access”

- **IT Service Provider on monthly retainer**
- **December 2016 IT Provider identifies attempted access via Remote Access Program**
- **January 2017 upgrades Remote Access to VPN**
- **February 2017 returns rejected**
- **IT forensics reveal remote access compromise via employees infected home computer in 03/16**
- **Perpetrator loaded hidden program granting full access and capable of copying and extracting files**
- **Program concealed using a common file naming convention went undetected from 03/16 to 02/17**
- **1/3 of clients ID Theft Victims**

207.96... [Full Info]	CA	Quebec	Montreal	Server 2008 R2	11.25 GB	119.82 Mbit/s	95.1 Mbit/s	x	x	28.02.2017	UFOSystem	54.50
207.253... [Full Info]	CA	Quebec	Quebec	Windows 10	63.96 GB	21.9 Mbit/s	9.42 Mbit/s	x	x	18.04.2016	solomon	53.25
69.70... [Full Info]	CA	Quebec	Dolbeau-mistassi...	Server 2012 R2	15.96 GB	27.25 Mbit/s	12.6 Mbit/s	x	√	22.01.2017	Zeuz	50.25
24.37... [Full Info]	CA	Quebec	Montreal	Server 2012 R2	31.75 GB	37.86 Mbit/s	23.59 Mbit/s	x	x	18.01.2017	Obama	50.25
72.143... [Full Info]	CA	Ontario	Collingwood	Server 2008	4 GB	25.39 Mbit/s	4.39 Mbit/s	x	√	29.01.2017	Re-Selling	50.00
62.49... [Full Info]	GB	England	Bexleyheath	Windows 7	3.42 GB	17.59 Mbit/s	37.8 Mbit/s	x	√	03.02.2017	Re-Selling	50.00
69.70... [Full Info]	CA	Quebec	Montreal	Server 2008 R2	100 GB	20.72 Mbit/s	9.45 Mbit/s	x	x	23.08.2016	Obama	49.25
24.37... [Full Info]	CA	Quebec	Quebec	Server 2008 R2	31.97 GB	32.45 Mbit/s	17.24 Mbit/s	x	x	17.01.2017	Obama	49.25
74.57... [Full Info]	CA	Quebec	Riviere-beaudett...	Server 2008 R2	31.91 GB	25.73 Mbit/s	4.62 Mbit/s	x	x	18.01.2017	Obama	49.25
50.27... [Full Info]	US	Texas	Lubbock	Server 2008 R2	15.96 GB	54.55 Mbit/s	6.1 Mbit/s	x	x	26.11.2016	selez	49.25
58.108... [Full Info]	AU	Western Australi...	Perth	Windows 10	3.69 GB	14.2 Mbit/s	504 Kbit/s	x	√	27.01.2017	AutoBot	49.00
74.50... [Full Info]	CA	Quebec	Montreal	Windows 8.1	7.89 GB	57.32 Mbit/s	15.68 Mbit/s	x	x	30.01.2017	Zeuz	47.00
58.108... [Full Info]	AU	Queensland	Gold Coast	Windows 7	2.99 GB	3.14 Mbit/s	144 Kbit/s	x	x	21.07.2016	UFOSystem	47.00
24.157... [Full Info]	CA	Quebec	Brossard	Windows 7	11.99 GB	35.59 Mbit/s	17.24 Mbit/s	x	√	22.02.2017	UFOSystem	47.00
47.221... [Full Info]	US	Texas	Kingwood	Windows 10	3.0 GB	26.13 Mbit/s	2.73 Mbit/s	x	√	05.02.2017	Re-Selling	47.00
58.108... [Full Info]	AU	Western Australi...	Perth	Windows 7	2.34 GB	5.67 Mbit/s	688 Kbit/s	x	√	22.01.2017	sigaj	47.00
173.176...							12.6					

Protect

Add Funds Tickets

Search

United States

Choose Provider

Direct IP

TRY#	REGION, STATE
3	Florida
3	Florida
3	Florida

US 71.251...
 Florida, Tampa | ZIP: 33601
 Verizon FiOS

Checked	Uptime
06.02.2017	06 Hours

1333.00\$

Windows 7 | x64 | EN
 AMD A10-5800K APU with Radeon(tm) HD...
 Ram. 7.19 GB | CPU Cores. 4

24.87 Mbit/s 18.9 Mbit/s

Check IP-Score (0.20\$)

Admin Privilege: **Yes**
 Direct IP: **No**
 Antivirus: **Unknown**
 Browsers:
 Blacklist: **0 / 5**
 Opened Ports: **No**
 Virtual: **No**
 Ransomware: **No**

Payment Systems

1. chaseonline.chase.com
2. chase.com
3. suntrust.com
4. wells Fargo.com
5. paypal.com

Poker Systems

Not Found.

Internet Shops

1. verizon.com
2. sprint.com
3. officedepot.com
4. verizonwireless.com
5. capitalone.com
6. sears.com
7. qvc.com
8. lowes.com
9. target.com
10. bhphotovideo.com
11. ebay.com
12. amazon.com
13. walmart.com
14. bestbuy.com

Dating Sites

1. match.com

Settings Logout

Search

LAST CHECK*	SELLER
06.03.2017	canonxp
07.03.2017	Obama
06.02.2017	sigej

Detect

Install and update anti-virus, -spyware, and other –malware programs

Maintain and monitor logs

<https://www.youtube.com/watch?v=RJJEyGkS9jA>

Protect (Phishing Emails)

From: **Posing as Outside Private Sector Entity**

Date: Thu, Jun 22, 2017 at 10:54 AM

Subject: Database Error

To: **Tax Practitioners**

In our database, there is a failure, we need your information about your account.

In addition, we need a photo of the driver's license, send all the data to the letter. Please do it as soon as possible, this will help us to revive the account.

- *Company Name *
- *EServices Username *
- *EServices Password *
- *EServices Pin *
- *CAF number*
- *Answers to a secret question*
- *EIN Number *
- *Business Name *
- *Owner/Principal Name *
- *Owner/Principal DOB *
- *Owner/Principal SSN *
- *Prior Years AGI

Phishing E-mail (Continued)

From: SimonandMelisa Willetts [<mailto:willettssimonandmelisa@gmail.com>]
Sent: Monday, February 20, 2017 6:58 AM
To: Tax Practitioner
Subject: Re: Our 2016 Taxes

My wife and I should have all our 2016 docs in a week or two.

Last year we moved from Wyomind DE ~ Mr Pryor was our previous CPA.

Here is our 2015 Tax Documents for your review.
However, we can be on a call Friday 10AM ~ OK?

Simon & Melissa Willetts Shared - Tax Documents

<<http://rktaxprep.info/customers/Pryordocs2015/pdf/>>

On Fri, Feb 17, 2017 at 8:45 PM, Tax Practitioner wrote:

Good morning Simon & Melisa,

Yes, I am accepting new clients. Are you in the City area?
Would you like to set up a time to meet?

Phishing E-mail (Continued)

From: Tax Software Company
Sent: February 13, 2017 12:16 PM
To: Tax Professional
Subject: Access Locked

Dear Customers ,

Access to Tax Software has been suspended due to error(s) in your security details.

Follow the link below to unlock your access

[Unlock](#)

Thank you.

© Copyright 2017 Tax Software. All rights reserved.

Phishing E-mail (Continued)

From: **Impersonating a Software Company**
To: **Tax Practitioner**
Sent: 8/10/2016 7:14:26 A.M. Eastern Daylight Time
Subj: Software Update Notification (Do NOT Reply)

Software Company Product Notification System

Dear Client,

Please DO NOT Reply to this e-mail.

All replies to this address will not be received by **Software Company**.

Please download and install this important update to your computer.

[Click Here](#)

Thank you for using **XXXXXX** Software.

-Customer Support.

Phishing E-mail (Continued)



Dear User:

Your e-services account is secure. We are doing a one time verification to your e-mail. This will work as a recovery in case your account is compromised. Click or copy the link below to your browser to complete this process.

https://la2.www4.irs.gov/pub/rup_login_1?TYPE=33554433&REALMOID=06-3e42c2f4-1c41-0019-0000-25b0000025b0&GUID=&0000--4d5700004d57%26GUID%3d%26SMAUTHREASON%3d0%26METHOD%3dGET%26SMAGENTNAME%3dlqjzN0Exzjq7GXjalQAtum2VjVbftpJfXjCX5EEznNQ6gB2VzGstn8fCh3KSapr%26TARGET%3d--SM---%2fPORTAL----PROD-%2fCRM-%2fsignon-%2html

If you need any assistance with changing your password, please read the e-services FAQ. On-line assistance is also provided within the Change Password function.

Detect

Practitioner Breach 3 “Malware”

- **Tax practitioner opens E-Mail with attachment and clicks on attachment.**
- **IT Forensics reveal hidden program granting access was loaded when the attachment was opened**
- **Malware and key logger were downloaded on network**
- **Users on the network logged into various portals which allowed the username and passwords to be accessed.**
- **Perpetrators were able utilize the username and passwords to gain full access to financial information.**

Respond

Develop a plan for disasters and information security incidents

- **The plan should include the following Roles and Responsibilities:**
 - **Who makes the decision to initiate recovery procedures and contact law enforcement.**
 - **What to do with your information systems (i.e. shut down/lock computers, move to backup site).**
 - **Contact IRS and State Tax Authorities.**
 - **Who to call in case of an incident (i.e. How and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers, or insurance providers).**
 - **State Notification Laws.**

Respond

IRS

Tax professionals should contact IRS Stakeholder Liaison when a compromise is detected. The Stakeholder Liaison will refer Information within IRS (i.e. Criminal Investigations, Return Integrity & Compliance Services)

<http://www.irs.gov/Businesses/Small-Businesses-&Self-Employed/Stakeholder-Liaison-Local-Contacts-1>

State Tax Agencies

Tax professionals can e-mail the Federation of Tax Administrators to get information on how to report victim information to the appropriate state authorities.

StateAlert@taxadmin.org

Recover

- **Make full backups of important business data/information**
- **Make incremental backups of important business data/information**
- **Make improvements to processes / procedures / technologies**

Recover

Practitioner Breach 4 “Ransomware”

- Delivery of the ransomware came in the form of phishing e-mail to the human resource manager.
- Manger clicked on the link and ransomware was installed onto the network.
- Ransomware shutdown the system and demanded payment of \$1,500 in Bitcoins.
- Perpetrators threatened to sell the PII on the dark web.
- Tax practitioner paid \$1,500 and had IT specialist remove and restore the data using backup tapes.

Cyber Security Resources

- Internal Revenue Service (IRS) Publication 4557
 - <https://www.irs.gov/pub/irs-pdf/p4557.pdf>
- **IRS RESOURCES for Tax Professionals**
 - <https://www.irs.gov/for-tax-pros>
 - **Latest News Protect Your Clients; Protect Yourself**
 - <https://www.irs.gov/individuals/protect-your-clients-protect-yourself>
- Federal Trade Commission
 - <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security>
 - FTC Start with Security
- National Institute of Standards and Technology (NIST)
 - <https://www.nist.gov/>
 - Small Business Information Security: *The Fundamentals*
 - <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Questions?