NATP™ National Association of Tax Professionals

Identity Theft 2 – Practitioner
Your Office: Securing Your “Goldmine”

Through Real World Examples

A Guide to Building Your Own
Written Information Security Plan (WISP)
Larry L Gray, CPA, CGMA

I Just Want To Do A Tax Return

How did we get here?

- 1967 Paper
- 1977 Courier Service
- 1987 Best of Breed
- 1997 Virtual Office Beta Test
- 2007 Integration
- 2017 Information Security

Internet of Things

Where are we going…

My “goldmine” is secured

“I can once again just do a tax return.”

Identity Theft Opportunities

Your Office

Cloud Storage

Incoming Email

Malware

Back-up Drives

Tax Software

A Disgruntled Employee

Phishing Emails

Clients' Payroll Software

Accounting Software

Working From Home

Wi-Fi Security

Paperless Office

Janitor

Employees

Clients' QuickBooks

The Internet of Things

Estimated to consist of almost 50 billion objects by 2020

Heating Systems

TVs

Video Cameras

Wearable Devices

Coffee Makers

Headphones

Microwaves

Thermostats

Copiers

Scanners

Laptops

Postage Meters

Bluetooth

Stereos

Vacuums

tablets

Wi-Fi

Vehicles In Your Parking Lot

Calculators

Vending Machines

Security Cameras

Elevators

Lamps

Monitors

Desktops

Gaming Systems

Alarm System

Cellphones

Refrigerators

Routers

Printers

Projectors

Water Dispensers

Buildings Next Door

The Goldmine

How Many Years of Info?

Bank Statements

Community

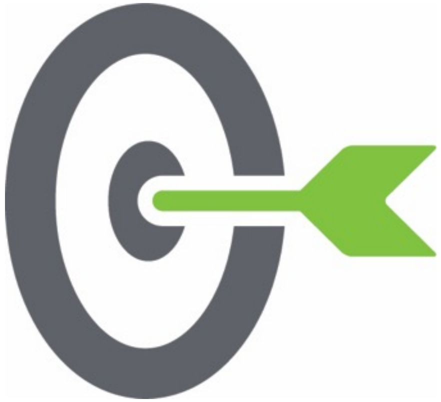
Driver’s License

Investment Accounts

1120s

Preparer Notes

Medical Records



1099-INT

1099-DIV

Addresses

1040s

Ledgers

Kids’ Information

Birthdays

Contracts

Social Security Card

Know The Law

- Gramm-Leach-Bliley Act
- Commission’s Privacy Policy 16 CFR §313.3(k)(viii)
- Federal Trade Commission Financial Privacy & Safeguards Rule

“…all businesses regardless of size, that are “significantly engaged” in providing financial products or services…professional tax preparers…”

“…requires companies to develop a written information security plan that describes their program to protect customer information.”

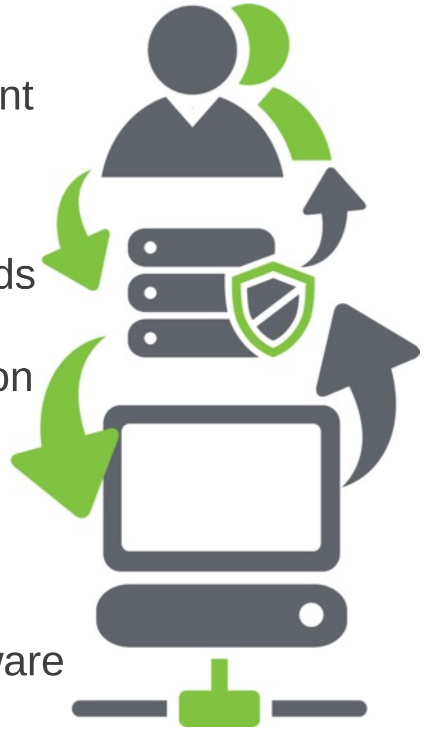
I Just Want To Do A Tax Return

Paper

client

Office
Tax Software

Security Toolbox



client

Firewall
passwords
IDS/IPS
Encryption
Portal
WISP

Office
Tax Software

Cyber Security Best Practice Basics

- Segment networks; separate sensitive information from public networks
- Firewalls (properly configured)
- Good intrusion detection systems (IDS)
- Regularly updated antivirus and anti-malware software
- Encryption: storage, transmission, and when logged out
- Strong passwords changed frequently
- Secure, encrypted back-up
- Strong 3rd-party vendor security policies
- Have a Written Information Security Plan (WISP)

Policy Development and Management

A pledge to your clients to protect their information.

- Have a Written Information Security Plan (WISP)
- Review policies and procedures of the WISP at least annually
- Evaluate your risk and assess vulnerabilities
- Establish security roles and responsibilities
- Determine best practice
- Establish strong password policies
- Designate a Security Coordinator

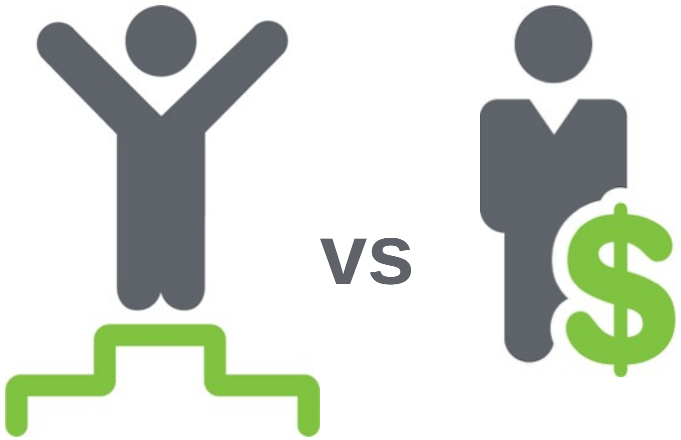
Security Coordinator’s Role

Good communication skills are a must.

- Train employees on their security-related rolls and responsibilities
  - Avoid social engineering and phishing attempts
- Assure employees have a copy of your Written Information Security Plan
  - Get signature proof they have read it and understand it
- Heed credible security warnings and move quickly to fix them
  - Regularly install patches that resolve vulnerabilities
- Periodically test your WISP safeguards
- Practice strong security measures and your staff will follow your lead

Operational Security

- Identify your most valuable processes and assets
  - Assess risks and safeguards in place
- Determine risk’s impact vs. extra cost of counter measures
- Have specific security plans in order to minimize damage physically, financially, and reputationally



Facility Security

Security training should be stressed as critical and reinforced via daily procedures and leadership modeling.

- Lock file cabinets/doors when unattended
- Keep a careful inventory of your company’s computers
- Maintain secure, encrypted backup records
- Dispose of trash securely
- Dispose of electronic equipment securely
- Train your employees

Network Security

- Segment networks
  - Separate sensitive information from public networks
- Use several layers of security
  - Put sensible access limits in place
  - Everyone use hard to crack passwords and protect them
- Computers and devices should encrypt all data, even when a user is logged out
- Increase the safety of your system: keep it up-to-date

Website Security

- Web servers open a window between your network and the world
- One of your most serious sources of security risk
- Essential to keep software up-to-date
- Configure new servers and change default settings

Wireless Security

- Understand how your wireless network works
  - Unauthorized activity could be traced back to your account
- Secure your router
  - It’s your first line of defense for guarding against attacks
- Use encryption on your wireless network
  - Wi-Fi Protected Access (WPA2) is the strongest
- Secure and limit access to your network
- Keep WLAN for guests separate from main company network

Email Security

- Set up a spam email filter
  - Email is the primary method for spreading viruses and malware
- Train your employees to identify malicious emails
  - Don’t open attachments in emails unless you know who sent it and what it is
- Add encryption capabilities to emails, and enforce this policy with employees

> *“…90% of information security problems would go away if people stopped clicking on links in email.”*
>
> Jason Thomas, Chief of Innovation, Thomson Reuters Special Services

Mobile Device Security

Train your employees: Treat mobile devices like a personal computer

- Use security software
- Automatic software updates
- Encrypt the data; configure it properly
- Use strong password protection
- Set “what to do” if lost or stolen
- Wipe them clean before disposal

- Employ these strategies for email, texting and social media
    - Avoid opening unexpected text messages from unknown senders
    - Don’t be lured in by spammers and phishers
    - Click with caution

“It is important to remember that while the individual employee may be liable for a device, the company is still liable for the data.” - Federal Communications Commission, *Cyber Security Planning Guide*

Employee Security

Identity theft prevention must start at the employee level

- Develop a hiring process to properly vet candidates
  - Check references and/or do background checks before hiring
- Provide security training for your employees
  - All must sign an agreement to follow company policy in securing data
- Set appropriate access controls for employees
  - Only grant access to those who need that information to do their jobs
- Evaluate your employee exit strategies
  - Close terminated employee accounts and remove their access to data

Your Written Information Security Plan

Getting Started

- Secure your clients’ personally identifiable information
  - Document security measures; update regularly
- Data Breach – Response and Recovery
  - **Who** – your Security Coordinator
  - **What** – steps to take next
    - Secure info not compromised
    - Do not destroy evidence
  - **When** – to report the breach
    - Notify Feds, State, Local officials
    - Notify clients

Actions When Compromised

- Contact IRS Stakeholder Liaison when compromise detected
  - https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts-1
- Stakeholder Liaison will refer information within IRS
- Follow state reporting requirements
- Report compromise to FBI, US Secret Service, Federal Trade Commission
- Get your ducks in a row…
  - Post information on your website
  - Set up a call center for complaints and concerns
  - Offer credit protection services for those affected
  - Consider offering 1 year of fraud prevention services to those affected
- Start rebuilding your practice

Tax Professionals Cybersecurity Resources

- Federal
  - www.identitytheft.gov
- Internal Revenue Service
  - www.IRS.gov/identitytheft
- Federal Trade Commission
  - https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- IRS Resources for Tax Professionals
  - https://www.irs.gov/for-tax-pros

What to Look for in an IT Security Professional

IT Security Professional

- Certified Information System Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- A person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security Institute (SANS)

Questions to Ask An IT Security Professional

Be security literate enough to ask questions and know if the answers make sense.

1. What is the difference between IT and Cybersecurity IT?.
2. What should I have to protect me from ransomware?
3. If ransomware gets in, what should I do?
4. What is the difference between a portal and an email?
5. How large is a typical security check list and how many have you done?
6. What Best Practice did you go by?
7. Remember – You cannot transfer your responsibility to a 3rd-Party

NATP™ National Association of Tax Professionals

Contact Information

Member Services: 800.558.3402, ext. 3
Email: natp@natptax.com
Federal Tax Research: 800.558.3402, ext. 2
Website: natptax.com