Cybersecurity Update

VanderWal Agency LLC

“Peace of Mind Comes With A Plan”

Objectives

- This course is designed to provide insurance professionals an overview and general understanding of cyber security protocol and assessment guidelines involving loss of customer data.

Objectives

- A discussion of the regulatory environment, risk assessment protocol and notification rules offers agencies a framework for managing data and assessing compliance issues.
- Quick tips for administrative, technical and physical data protection as defined under Gramm Leach Bliley are reviewed.

Predators and Criminals

Why cyber security?

Administrative, Physical and Technical

Critical information

"***Our identity is*** *increasingly going to become the* ***asset*** *that we have to be most* ***careful to protect in the 21st century*** *where the ability to get information, move it around the world and store it indefinitely creates greater and greater risks to personal reputation and personal privacy"...*

--Homeland Security Secretary Michael Chertoff
August 2008

Everyday we share…

October- National Cyber Security Month

Own IT, Secure IT, Protect IT

Own it

Never Click and Tell

Staying safe on social media

Update Privacy Settings

Keep Tabs on Your Apps

Best practices for device applications

Secure it

Shake Up Your Passphrase Protocol

Create strong, unique passphrases

Double Your Login Protection

Turn on multi-factor authentication

Secure it

Shop Safe Online

Play Hard To Get With Strangers

How to spot and avoid phish

Don’t bite on Phish

Laurie VanderWal

From: Joseph Morgan <joseph@rogers.com>
Sent: Thursday, July 6, 2017 11:39 AM
To: laurie@vanderwalagency.com
Subject: RE:RE: shipping information

Hello,

The delay happened because of the Independence Day.
Here is the label from UPS, use the tracking number on their website :

h ttps://www.ups.com/WebTracking/track?loc=en_us&action=view&id=728082 64&acc=laurie

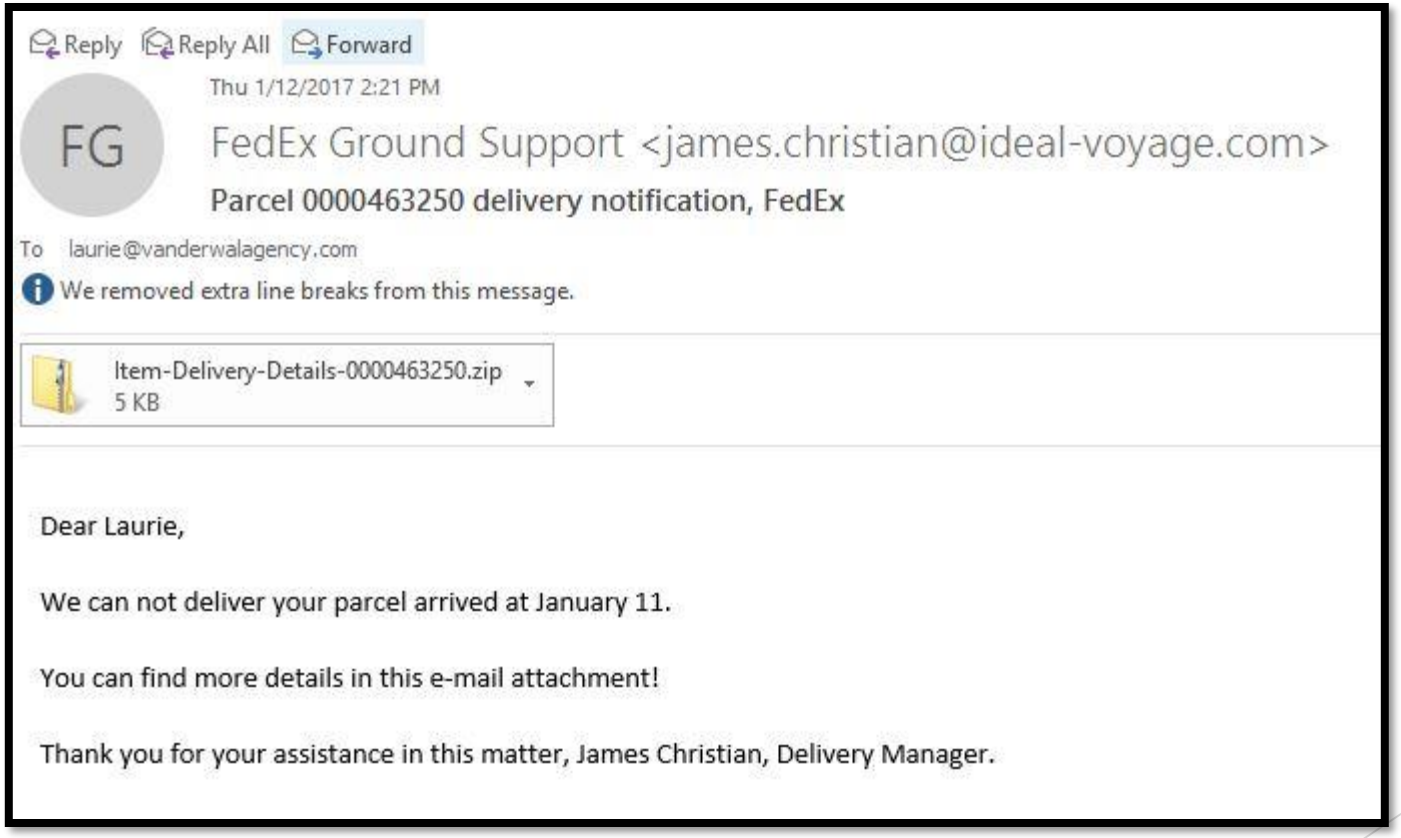
Thank you again for your patience!

Joseph Morgan
Orders Manager
email:joseph@rogers.com
tel.:726-215-7001

On Mon, Jul 3, 2017 at 3:21 PM, <laurie@vanderwalagency.com> wrote:

> Have you shipped my order?
> Give me a call as soon as possible.

Don’t bite on Phish



Reply Reply All Forward

Thu 1/12/2017 2:21 PM

FG

FedEx Ground Support <james.christian@ideal-voyage.com>

Parcel 0000463250 delivery notification, FedEx

To laurie@vanderwalagency.com

We removed extra line breaks from this message.

Item-Delivery-Details-0000463250.zip
5 KB

Dear Laurie,

We can not deliver your parcel arrived at January 11.

You can find more details in this e-mail attachment!

Thank you for your assistance in this matter, James Christian, Delivery Manager.

Protect it

If You Connect, You Must Protect

Stay Protected While Connected

Wi-Fi safety

Protect it

Keep updated security software

Use current web browser and operating systems

Protect it

Business must keep customers, consumers, and staff information safe

If You Collect--It Protect It

Accidental release

Intentional data breach

Unauthorized access of information

Contractual relationships

Regulatory

Federal & State

Health & Human Services

NAIC

Federal Trade Commission Workshop Voice Cloning Technology

- Speech synthesis
  - Using the voice of an actual person
- Development and use of voice cloning technologies
  - Healthcare
  - Consumer-oriented applications
    - Virtual assistants
  - Customer service
  - Entertainment
  - Carry out fraudulent schemes

Federal Trade Commission Workshop Voice Cloning Technology

- Ethical & legal concerns related to the use of cloned voices
  - Call to change a beneficiary
  - Increase life insurance amount
  - Remove cash from a financial services account
  - People may become predators!!

Regulating Protection of NPI

Financial Data Protection & Consumer Notification of Data Security Breach Act of 2006

NEBRASKA

Regulating Protection of NPI

Nebraska amended 2018

Added language for

Securing a Written Information Security Program (WISP)

Including proper disposal of data

NEBRASKA

Regulating Protection of NPI

Nebraska amended 2018

If you share NPI with third party vendor, it shall require by contract that the service provider implement and maintain reasonable security procedures and practices of that data.

NEBRASKA

Regulating Protection of NPI

Personal Information Security Breach Protection Act 2008

500 records or more within 5 business days

Regulating Protection of NPI

If you are required by other state or federal law with higher compliance standards, then you are likely compliant with Nebraska & Iowa state laws.

Regulating Protection of NPI--HHS

- Notification rules-HHS
- 500 records or more immediately
- 500 records or less annually

HHS Data Breach Notification Rule

HITECH

Designed to encourage healthcare providers to adopt electronic health records

Driven to improve privacy and security protections for healthcare data.

Financial incentives for adopting EHRs were offered

Increased penalties for violations of the HIPAA Privacy and Security Rules.

NAIC Cyber Security Model Law

National Association of Insurance Commissioners

NAIC Model Law

- Defines the framework for security
- Outlines the objectives
- Provides *Risk Assessment* protocol
- Implementation guidelines

NAIC Model Law

Incident response plan

Investigation and notification of a cyber security event

Oversight

- ✓ Board of Directors
- ✓ Third-Party Service Provider Arrangements

NAIC Model Law

- Long term goal of model law
  - Create a model framework for data protection
  - Offer guidelines for professionals to complete a *Written Information Security Program (WISP)*

States with NAIC Model Law

- Ohio
- Michigan
- Alabama
- Delaware
- Connecticut
- New York
- New Hampshire
- Minnesota
- Mississippi

Common denominator-Require a Written Information Security Program (WISP)

Risk management

- Errors & omissions coverage
- Cyber insurance
- Insurance carrier appointments
- Federal and state regulators

Common Denominator—Require a Written Information Security Program (WISP)

Risk Assessment Protocol

Where do we start?

Policy & Procedure

- Information access use policy
  - Do not use business computer for personal reasons
  - No online shopping on office computers
  - No personal downloads, ie music or entertainment

Policy & Procedure

- Mobile device wifi usage
  - Do you know if your mobile device automatically connected to an open wifi at our meeting today?
  - Is it important to know?
  - Why?

Policy & Procedure

- Mobile device
  - Do you know how to locate your phone if it were lost?
  - Do you need to notify anyone within your business sphere that the device is lost, MIA and/or may be open to compromise?

Staff training

- Play a game, compliance can be fun!
- Locate your phone game
  - Put all phones in one room
  - Go back to your desk
  - First phone to ring wins!
    - Choose a prize as you go down the line
    - Last one in gets to write the policy and procedure on lost phone consequence!!

Policy & Procedure-Password Management

- What is your password management system?
  - Manual
  - Software driven
    - Password vendors
    - Identity theft product security
- Does it look different?
  - Personal
  - Business

Policy & Procedure-Password Management

- Do you have a password to get into your mobile device?
  - DNA
  - Facial
  - Fingerprint
  - Designed pattern
  - Set of unique numbers

Policy & Procedure

- Are you using multi-factor authentication?
- Do you have a system for creating, changing, and deleting passwords?
- If you choose a manually driven method
  - Make it a game

Staff training

- Play a scrabble password game
  - Create passwords from game words
  - Be creative, have fun
- Create a new alphabet
  - Replace letters for numbers
  - Make every letter “A” the number 3

Policy & Procedure

- Vendor risk management
  - Set protocol for access
  - Review contractual relationships
  - Obtain cyber security insurance certificate
    - WISP

Policy & Procedure

- Review social media protocol and presence
  - Should business information be allowed on personal social media accounts? Ie, an employer's name
  - Are staff posting content that violates the company ethics code?
    - Have you ever discussed an ethical code for online posting with staff?

Policy & Procedure

- Review social media staff presence
  - Are defamatory statements being made? About anyone?
  - Are the ethics of the company being upheld by the individuals?
  - What common sense rules should we follow?
  - What posting is appropriate?

Staff training

- Define the culture of your organization for security
- Discuss guidelines for an online ethical code of conduct
  - Personal
  - Business

Social media and Underwriting

What does the future hold for consumers as we look to underwrite social media content?

Future Underwriting

- Is it OK for a high-profile city employee to put out a video post showing themselves “burning” up the block
- From 0 to 60 in 4.3 seconds
- Should that type of activity reflect in their auto insurance rate?

Future Underwriting

- Is it OK for an individual applying for life insurance to flaunt a risky online lifestyle?
  - What is risky?
  - What do underwriting guidelines state?
- Could that same behavior by the city employee increase the chance for an untimely death?

Social media profile

- Household & individual profile
- Category of content posting

- ✓ Influencer
- ✓ Volunteer activity
- ✓ Gets along with others
- ✓ Supports community
- ✓ Financially sound
- ✓ Responsible
- ✓ Very socially active
- ✓ Alcohol related events
- ✓ Unpopular comments
- ✓ # of post dislikes
- ✓ Size of friend base
- ✓ Risky behavior
- ✓ Antagonist behavior
- ✓ Business posting

Future Policy & Procedure

- Online presence matters
- Social media posting
- Social media pictures
- Business networking platforms
- Local neighborhood online groups

Breach Protocol

What to do before, during and after the breach

After the breach

- The first hour
- The first 24 hours
- Week one after a breach
- One month after a breach

Tick, tock…Tick, tock…

Incident Response

- Internal notification
  - Policy on what to communicate
  - Proactive stance
- Customer notification
- Insurance carrier notification

Threat analysis-Technical

- Forensic analysis
  - IT department
  - Cyber insurance resource
    - Recommendations
      - National
      - Local resources

Threat analysis-Technical

- Technology safeguards protocol review
- Known Malware
- Antivirus compromised
- Current security protocol
  - Is it 8 am or 5 pm?
  - Is it payday or an average day?
- Backup protocol

Threat analysis-Physical

- Physical security checklist
- Building vulnerabilities
- Windows compromised
- Missing property

Incident Response

- Identify breach type
  - Physical
  - Network security
  - Internal/employee
  - Cloud based
  - Intentional
  - Unintentional
  - Hard copy paper

Incident response

- Notify law enforcement
- Work cohesively with technical and leadership teams to limit damage
- Notify customers
- Notify any regulatory bodies
- Begin the recovery effort
- Hold a “lessons learned” meeting

Cyber Insurance review

- Cyber policy coverages and guidelines
  - Victim credit monitoring
  - Notification reimbursement
  - Forensic analysis
  - First or third party liability

Gramm Leach Bliley & The Circle of Data

Collection, Storage, Access, Protection, Destruction

Defining NPI

- Compliance policy on protecting data
  - Customer
  - Employee
  - Corporate business information

Collection of NPI

- Identify the elements for protection
  - Social security number

  - Financial data
    - Credit/debit card
    - Checking account

  - Birthdate
  - Driver's license
  - Application information

Collection of NPI

- Identify the elements for protection
  - Medical information
  - DNA
  - Fingerprint
    - Handprint
  - Facial recognition
    - Iris scan
  - Voice recognition
    - Virtual assistants

Collection of NPI

- Identify the elements for protection
  - Employee records
  - Proprietary corporate details
  - Customer database
  - Intellectual property
  - Financial statements
  - Architectural plans

Collection of NPI

Identify all opportunities for incoming data

- Electronic
  - Mobile device
  - Website
  - Social Media
  - Email
- Paper
- Physical business office

Storage of NPI

- Electronic security
  - Desktop protocol
  - Mobile device protocol
- Paper records

Accessing NPI

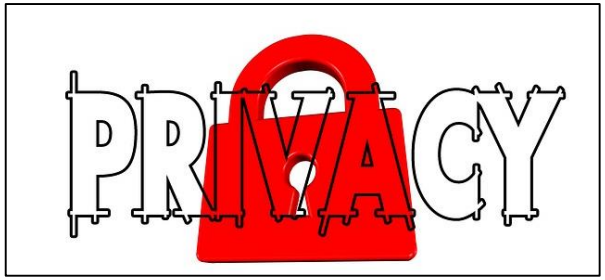
- A google search can be revealing
- COMMERCIAL GENERAL LIABILITY
  - CG 00 01 04 13

Accessing NPI

- Google searching creates vulnerabilities
- COMMERCIAL GENERAL LIABILITY
  - CG 00 01 04 13

Accessing NPI

- Identify unauthorized use of information
  - Staff permission levels
    - Property/casualty agents
    - Life/health agents
    - Medical information protocol
    - Financial services records



Accessing NPI

- Compliance and internal systems
  - Internal messaging platforms
    - Virtual assistant
  - Personal functions on business computer
    - Personal email access
    - Social media access

Email

IT & Accessing NPI

- IT and cloud accessibility
  - Who controls storage and access?
  - How is data accessed and storage managed?
  - How long is information accessible?
  - When is data overwritten with new information?

Outside Access to NPI

- Outside office accessibility
  - Mobile device/Tablets
  - Laptops
  - Personal home computer and personal mobile devices
- Unsecure wifi network vulnerability

Protecting data

- Secure your wifi
- Don’t share passwords
- Review protocol on a regular basis
  - Security is an ongoing moving target

Destruction of data--NPI

- Electronic and paper destruction policy
- Retention policy
  - Insurance carrier
  - State department of insurance
  - Internal company policy

Personal information

IT'S LIKE MONEY
RESPECT IT
PROTECT IT!

Your words are permanent

TMI

Thank you for attending

VanderWal Agency LLC

Laurie VanderWal

“Peace of Mind Comes With A Plan”

402-216-8262