

Cyber Security Summit

"I am convinced that there are only two types of companies – those that have been hacked and those that will be... and even they are converging into one category – companies that have been hacked and will be hacked again."

– Robert S. Mueller, Director – FBI (2012)

The words of the former FBI director are alarming, yet accurate. Cyber-crime is an epidemic that is targeting the attorneys of North Carolina. Collectively, as a profession, we need to protect ourselves and our clients.

Investors Title Insurance Company, Lawyers Mutual Insurance Company, the North Carolina State Bar, and the Federal Bureau of Investigation have teamed up to present the **CYBER SECURITY SUMMIT**.

***False Sense of Cyber Security
It Could Not Happen to Me?***

Jonathan W. Biggs, Vice President Risk Management & Education

Cyber Security Summit – January 2017

Investors Title
INNOVATIVE BY INSTINCT



Investors Title
INNOVATIVE BY INSTINCT

Innovative by Instinct

***False Sense of Cyber Security –
It Could Not Happen to Me?***

Jonathan W. Biggs, Vice President Risk Management & Education

Cyber Security Summit – January 2017

False Sense of Cyber Security – It Cannot Happen To Me!

Jonathan W. Biggs, J.D.

Vice President of Risk Management & Education
121 North Columbia Street | Chapel Hill, NC 27514
P.O. Drawer 2687 | Chapel Hill, NC 27515
Main: 919.968.2200 | Direct: 919.945.2597 | Fax 919.968.0728
JBiggs@InvTitle.com | www.InvTitle.com

Investors Title
INNOVATIVE BY INSTINCT

3 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

False Sense of Cyber Security –

It Cannot Happen To Me!

- 1) Introduction
- 2) Cyber-Fraud Generally
- 3) Myths About Cyber-Fraud
- 4) Realities About Cyber-Fraud & You
- 5) Who Are the Criminals Today?
- 6) How Do Criminals Gain Access?
- 7) Actual Stories About Types of Cyber-Fraud
- 8) So What Do I Do
- 9) Cyber-Fraud Insurance

Investors Title
INNOVATIVE BY INSTINCT

4 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

DISCLAIMER

NO CLAIM IS MADE TO THE OWNERSHIP OF THE IMAGES OR EMAILS OF:

- **Master Yoda**
- **Emperor Palpatine**
- **Mark Hamill**
- **Any Star Wars Character**
- **Tom Cruise**
- **Jack Nicholson**
- **Robert Mueller**
- **Winston Churchill**
- **Arnold Schwarzenegger**
- **Matthew Broderick**
- **Jeffrey Jones**
- **Wayne Knight**
- **John Podesta**
- **Queen Victoria (on the stamp)**
- **Countless Fraudsters**
- **Cartoons & Other Images**

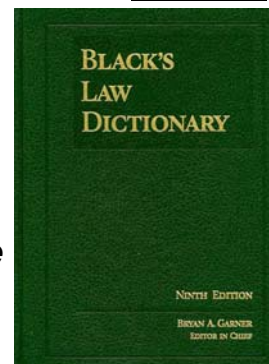
ALL ARE USED FOR EDUCATIONAL PURPOSES
UNDER THE FAIR USE DOCTRINE

Investors Title
INNOVATIVE BY INSTINCT

Introduction

What is Fraud?

- A **false representation** of a material of fact— whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed—
- is **intended to deceive** another
- so that the individual **will act** in reliance upon it
- that, in fact, **deceives** and
- to her or his **legal injury** (**DAMAGE**)



Investors Title
INNOVATIVE BY INSTINCT

What is Fraud Prevention?

- Fraud deterrence is the proactive identification and removal of the causal and enabling factors of fraud.
- Fraud deterrence is based on the premise that fraud is not a random occurrence; fraud occurs where the conditions are right for it to occur.
- Fraud deterrence attacks the root causes and enablers of fraud.
- This analysis could reveal potential fraud opportunities in the process, but is performed on the premise that improving organizational procedures to reduce or eliminate the causal factors of fraud is the single best defense against fraud.

Investors Title
INNOVATIVE BY INSTINCT

What is Fraud Deterrence?

Fraud deterrence involves both short term (procedural) and long term (cultural) initiatives.

What Are We Really Talking About?

- Professional & Ethical Representation
- Protecting Clients
- Avoiding Liability
- Avoiding Damage To Reputation

Investors Title
INNOVATIVE BY INSTINCT

What is CYBER - Fraud?

- Same as Fraud Generally
 - A **false representation** of a material of fact
 - is **intended to deceive** another
 - so that the individual **will act** in reliance upon it
 - that, in fact, **deceives** and
 - to her or his **legal injury** (DAMAGE)
 - **ADDITIONAL ELEMENT**
 - **Uses phone, computer or digital network to perpetrate the fraud**

What is CYBER - Fraud?

Cyber-Fraud is an all-encompassing term that includes a wide variety of types of fraud. It is often confused and identified with each of the sub-classes of Cyber-Fraud and used interchangeably.

False Sense of Cyber Security – It Cannot Happen To Me!

Cyber – Fraud Generally

What is Cyber - Fraud?

- When **DATA** or **INFORMATION** is stolen, the type of liability you have and the type of insurance that you need is referred to as **CYBER LIABILITY/DATA BREACH** insurance coverage.
- When **MONEY** is stolen, the type of liability you have and the type of insurance you need is referred to as **CRIME INSURANCE or CYBER THEFT INSURANCE** coverage.

Investors Title
INNOVATIVE BY INSTINCT

11 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Cyber – Fraud Generally

Cyber-Breach– **INFORMATION** STOLEN

The cyber-breach fraud can be perpetrated many ways, including the following:

- Gaining credentials (login and password) for access to a computer network that contains NPI;
- Intercepting un-encrypted or improperly encrypted communication containing NPI;
- Improper disposal of NPI;
- Sharing NPI with a source that is believed to be trusted (but is not); and
- Many more.

Investors Title
INNOVATIVE BY INSTINCT

12 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Cyber – Fraud Generally

Cyber-Theft or Cyber-Crime – **MONEY** STOLEN

- Cyber-Theft is what people generally think of when they think of Cyber-Fraud – someone stole **MONEY** from the trust account using the internet
- A separate flavor of cyber-fraud
- Needs to be explicitly covered by the insurance policy
- Crime Insurance or Cyber-Theft Insurance Policy.
- Involves a computer and/or a computer network in order to steal or misappropriate money.
- Log into your online banking and transfer funds to themselves.
- Many banks will not reimburse a business for money lost if the transfer is made with the correct account number, login, and password.

Investors Title
INNOVATIVE BY INSTINCT

13 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Cyber – Fraud Generally

C. Y. B. E. R.

Can

You

Be

Entirely

Ready ?

~~**Not Really**~~

NO!

But Try Anyway!

Investors Title
INNOVATIVE BY INSTINCT

14 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths

1. Birds will die if they eat the uncooked rice flung at newlyweds. **NOPE**
2. If you eat Mentos and drink Diet Coke simultaneously your stomach will explode. **Wrong Again. I Tried it!**
3. Carolina is a “Better Value” than Duke

Not According to US News and World Report

<http://www.usnews.com/education/best-colleges/articles/2015/09/01/2016-best-colleges-preview-top-10-best-value-schools>

Investors Title
INNOVATIVE BY INSTINCT

15 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #1 – Nobody Can Read My Emails

- Email Is Like a Post Card
- No Envelope

Investors Title
INNOVATIVE BY INSTINCT

16 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education



False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud **FALSE**

Myth #2 - Software Will Protect You

- Software alone is not going to stop cyber-crime. It is essential, but not the only thing you need.
- There is no more harmful notion than the one that leads people into doing whatever they want on their computers or smartphones because they have all of the latest software protections.
- Training is an absolute necessity.

Investors Title
INNOVATIVE BY INSTINCT

18 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

The only thing worse than training your employees and having them leave, is not training them and having them stay.

- Henry Ford



Investors Title
INNOVATIVE BY INSTINCT

19 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #3 – Using Encrypted Email Is All I Need to Protect Me from Cyber-Fraud

- The Encrypted Email May Come From or Go To The Wrong Address or Individual
- Check the Address on the Email Every Time.

Investors Title
INNOVATIVE BY INSTINCT

20 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #3 – Using Encrypted Email Is All I Need to Protect Me from Cyber-Fraud

- The Encrypted Email May Come From or Go To The Wrong Address or Individual
- Check the Address on the Email Every Time.

Investors Title
INNOVATIVE BY INSTINCT

21 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #4 – Once an Email is Encrypted, It Is Encrypted Forever

- Initiating an Email With Encryption Does Not Mean that Forwards or Replies Are Also Encrypted

Investors Title
INNOVATIVE BY INSTINCT

22 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #5 – Wiring Instructions Can Be Trusted If They Are Received By Encrypted Email or Fax

- Cyber Criminals Can Buy Fax Machines
- Cyber Criminals Can Send Encrypted Emails
- **Always** Verify Wiring Instructions With a Call Back to a Trusted Source
 1. Proper Identification
 2. Verbal Confirmation
 3. Delivery Verification

Investors Title
INNOVATIVE BY INSTINCT

23 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #6 – Changes In Wiring Instructions Is The Only Time That Warrants Call Back Procedures and Additional Caution

- A Change in Wiring Instructions Is Definitely a “Red Flag”
- **Always** Verify Wiring Instructions With a Call Back to a Trusted Source
 1. Proper Identification
 2. Verbal Confirmation
 3. Delivery Verification

Investors Title
INNOVATIVE BY INSTINCT

24 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Popular Myths About Cyber-Fraud

Red Flags

“Red Flags” are not absolute rules, but rather an indication that there may be something out of order with the wiring instructions. There may be reasons for the “Red Flag” that, upon proper investigation, may be very legitimate. However, you should look out for the following and investigate each instance of a “Red Flag” when they are discovered. Below is not an “all inclusive” list, but rather some of the more prevalent “Red Flags.”

Investors Title
INNOVATIVE BY INSTINCT

Popular Myths About Cyber-Fraud

Red Flags

RED FLAGS CONTINUED

- Wires to be sent outside of the United States
- Changes in Wiring Instructions
 - Very few individuals or corporations change their bank accounts in the middle of a transaction. Be very suspicious of change wiring instructions.
- Similar But Slightly Different Email Addresses
 - Many cyber criminals will attempt to defraud you by communicating with a very similar (but slightly different email address)
- Wire to a different geographic location than Recipient
- Wire to account which is not in the name of the Recipient

Popular Myths About Cyber-Fraud

Red Flags

RED FLAGS CONTINUED

- Individual Wire Sent to Corporate Account
- Corporate Wire Sent to Individual Account
- Broken English
 - Many cyber criminals are outside of the United States and English may not be their first language
 - Not an absolute, but worth checking out
- Unnecessary Speed Requirements or Demands
 - Everyone understands the desire to receive their money from a third party, but extraordinary pressure for the speed of the wire is generally a sign that they do not want you to investigate this “Red Flag.”

Popular Myths About Cyber-Fraud

FALSE

Myth #7 - Cyber-Crime Is Mostly About Credit Card Fraud

- The idea that cyber-crime is just about credit card fraud is a misconception that, ironically, can lead to credit card fraud and other forms of credit-related crimes.
- The majority of the cyber attacks are focused on grabbing personal identifying information from organizations that do business with a lot of people

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #8 - Cyber-Crime Is Only About Making a Buck

- If cyber-crime were only about making money, we would all be a lot safer than we are right now.
- Large numbers of hackers are driven by ideology.
- Many are far less interested in making money than in making money disappear are just reeking havoc by destroying information.

Investors Title
INNOVATIVE BY INSTINCT

29 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Myth #9 - Cyber-Criminals Don't Target Small Businesses

- Target was not really hacked
- The criminals hacked Target's HVAC vendor
- Looking for vulnerabilities on the Internet
- Do not be low hanging fruit

Investors Title
INNOVATIVE BY INSTINCT

30 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Popular Myths About Cyber-Fraud

FALSE

Myth #10 – My Errors & Omissions Insurance Will Cover Me for Cyber-Fraud

- General Liability and Errors & Omissions Policies generally have exclusions for Cyber-Fraud
- Confer with Your Insurance Agent About Cyber-Fraud Coverages
- There are Multiple Types of Cyber-Fraud Coverage

Investors Title
INNOVATIVE BY INSTINCT

Popular Myths About Cyber-Fraud

FALSE

Myth #11 – All Cyber-Fraud Insurance Is the Same

- Not All Cyber-Fraud insurance Coverage is the Same
- Ask Your Insurance Agent About
 - Cyber-Liability Fraud Insurance (Loss of Data)
 - Cyber-Crime Fraud Insurance (Loss of Money)
 - Social Engineering Fraud Insurance

Investors Title
INNOVATIVE BY INSTINCT

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Biggest Myth of All

***It Cannot Happen
To Me!***

Investors Title
INNOVATIVE BY INSTINCT

33 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

FALSE

Biggest Myth of All - *It Cannot Happen To Me!*

"There are only two types of companies:
those that have been hacked,
and those that will be."
Robert Mueller
FBI Director, 2012

Investors Title
INNOVATIVE BY INSTINCT

34 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #1 – Cyber-Fraud is Rampant



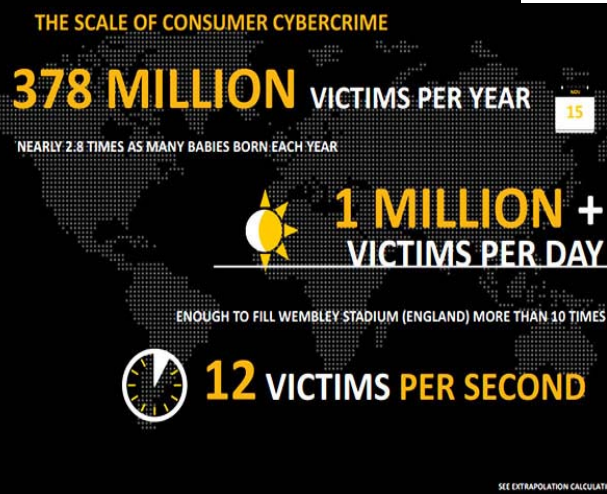
Investors Title
INNOVATIVE BY INSTINCT

35 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You



- 12 Per Second
- 720 Per Minute
- 43,200 Per Hour
- 345,600 During the Seminar
- 518,400 Before Lunch
- 1,036,800 Today

Investors Title
INNOVATIVE BY INSTINCT

36 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

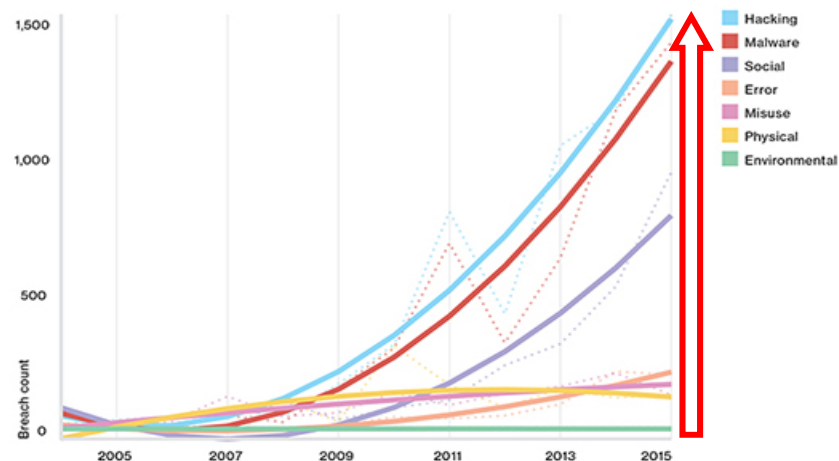


37 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Figure 4.

Number of breaches per threat action category over time, (n=9,009)



Source: Verizon 2016 Data Breach Investigations Report

38 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #2 – You Are A Target



Investors Title
INNOVATIVE BY INSTINCT

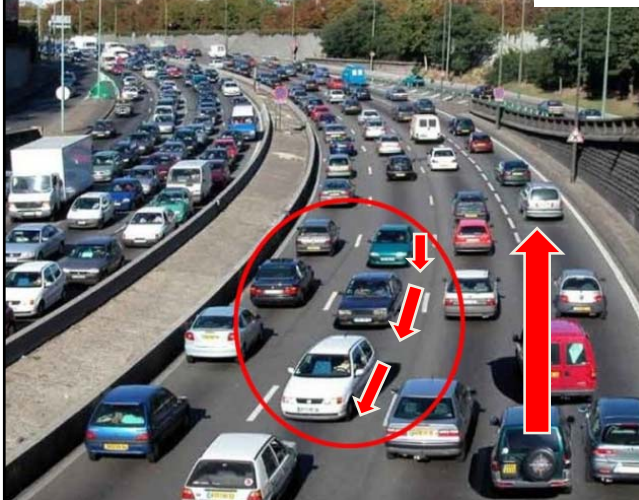
39 January 2017

False Sense of Cyber Security – It Cannot Happen To Me?

Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You



- Wrong Direction
- Only Road
- People Trying To Hit You
- Not Nimble Enough To Avoid Getting Hit
- No One Is!

Investors Title
INNOVATIVE BY INSTINCT

40 January 2017

False Sense of Cyber Security – It Cannot Happen To Me?

Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #3 – Social Media – a Hackers' Favorite Target

- 1.6 +/- Billion Social Network Users Worldwide
- 64% of Internet Users Access Social Media Online
- More than 600,000 Facebook accounts are compromised

EVERY SINGLE DAY

- Like-Jacking & Link-Jacking – Involuntary Redirects

Investors Title
INNOVATIVE BY INSTINCT

41 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

CYBER-FRAUD GOLD MINE

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #3 – Social Media – a Hackers' Favorite Target

Spouse's Name
Kids' Names
Parents' Names
Relationship
Favorite Food
Vacation Spots
Hometown
Your Birthday
Family Birthdays



Employment
Pets' Names
Your Schools
Kids' Schools
Hospital Visits
Dentist & Doctor
Success Stories
Life's Tragedies
& Rest of Your Life

42 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #4 – 99% of Computers are Vulnerable to Exploit Kits

- One or More of Oracle Java, Adobe Reader or Adobe Flash Resides on 99% of Computers.
- These Computers are Vulnerable to Exploit Kits
- Exploit Kits = Software Vulnerabilities
- Generally Due To Failure To Update
 - Software
 - Operating Systems
 - Anti-Malware Software

Investors Title
INNOVATIVE BY INSTINCT

43 January 2017

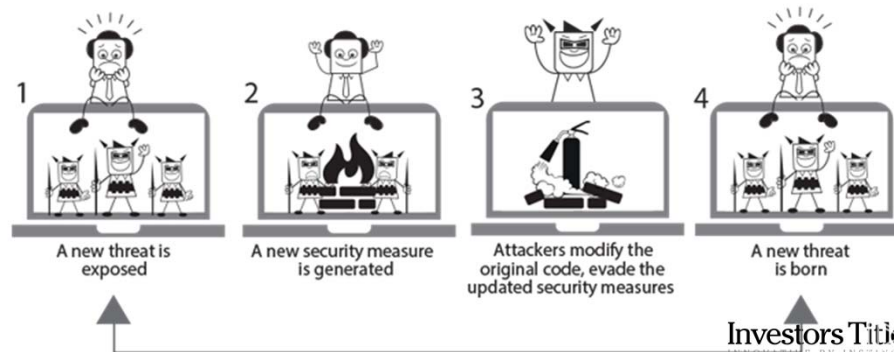
False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #4 – 99% of Computers are Vulnerable to Exploit Kits



Investors Title
INNOVATIVE BY INSTINCT

44 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Realities About Cyber-Fraud

Truth #5 – Insiders Biggest Cause of Cyber-Fraud

- Terminated Insiders - 59% of Employees Steal Proprietary Corporate Data when they quit or are fired
- Malicious Insiders are the least frequent, but have the potential to cause significant damage due to their level of access. Administrators with privileged identities are especially risky.
- Exploited Insiders may be “tricked” by external parties into providing data or passwords.

Investors Title
INNOVATIVE BY INSTINCT

Realities About Cyber-Fraud

Truth #6 – Funds Lost Are Tough To Recover

- 68% of Funds Lost as a Result of a Cyber Attack Are Declared Unrecoverable
- Must Act Quickly to Contact Bank and Authorities

Investors Title
INNOVATIVE BY INSTINCT

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #6 – Funds Lost Are Tough To Recover

- You Must Act **F.A.S.T.**
- You Need:
 - A Cyber-Fraud Response Team
 - A Cyber-Fraud Response Plan
 - To Keep Calm And Follow the Plan

Fast
Action
Stops
Theft

Investors Title
INNOVATIVE BY INSTINCT

47 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #7 – Your Old Cyber-Fraud Response Plan

1. Discover Breach or Loss
2. Panic, Curse & Throw Things
3. Cry
4. Call The Bank
5. Cry Again
6. Deny
7. Write a Big Check
8. Curse Again
9. Lose Sleep
10. Go To Dental School

**You Need
A New Plan!**

Fast **A**ction **S**tops **T**heft!

Investors Title
INNOVATIVE BY INSTINCT

48 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

FAST. FAST ACTION STOPS THEFT.

RESPONSE PLAN DOCUMENTATION

Investors Title
INNOVATIVE BY INSTINCT

STEP #1 – DO NOT PANIC

STEP #2 – Alert Internal Cyber Crime Response Team

Name	Phone	Email
1) _____	_____	_____
2) _____	_____	_____
3) _____	_____	_____

Date: _____ Time: _____

STEP #3 – Contact Bank(s)

Bank	Contact Name	Phone	Email	Last 4 of Account #	Date Contacted
1) _____	_____	_____	_____	_____	_____
2) _____	_____	_____	_____	_____	_____
3) _____	_____	_____	_____	_____	_____
4) _____	_____	_____	_____	_____	_____

CONTACT ALL OF YOUR BANKS – NOT ONLY FOR FINANCIAL LOSSES!
You do not yet know how invasive the breach/loss may be.

Date: _____ Time: _____

STEP #4 – File Report with IC3.gov – Internet Crime Complaint Center – FBI

- Complete the Attached Document Prior to Filing Report
- Print and Keep Copy of Complaint Filed

Date: _____ Time: _____

STEP #5 – Secure Your Office and Your Network

- Secure the Physical Premises ; Secure Digital Devices; Preserve Evidence; Stop Additional Loss
- Take Affected Machines Offline (but DO NOT TURN OFF) until forensics / IT has completed their investigation

STEP #6 – Document Specifics of Breach/Loss

- Complete the Attached Document
- Include ITIC W.I.R.E. Checklist, if a fraud involves a wire

49

itle
TINCT
ion



False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #9 – No Protection is Too Strong or Bulletproof

- Your protections must be appropriate to:
 - Your **size** and **complexity**
 - The **nature** and **scope** of your activities; and
 - The **sensitivity** of the **customer/client information** you handle.
- You must evaluate and adjust your protections in light of relevant circumstances, including changes in your business or operations, or the results of security testing and monitoring.

51

- Cost Will Always Be a Consideration and a Factor

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #10 – Cyber-Fraud Is Here To Stay

Stone Age	19 th Century	20 th Century	21 st Century
<ul style="list-style-type: none">• Fire• Wheel• Tablet• Chisel• No Money• No Secrets• Thief• <u>Criminals!</u>	<ul style="list-style-type: none">• Wood Stove• Horse Carriage• Electricity• Gold & Silver• Stamps• Radio• Horse Thief• <u>Criminals!</u>	<ul style="list-style-type: none">• Electric Stove• Car• Carbon Paper• Certified Checks• Overnight Delivery• Landline Phones• Organized Crime• <u>Criminals!</u>	<ul style="list-style-type: none">• Microwave• Hover board• Email• Wires• Video Chat• OnLine Banking• Cyber-Criminals• <u>Criminals!</u>

If You Use 21st Century Technology, You Must Protect Yourself Against Criminals with 21st Century Safeguards!

False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Biggest Truth of All – Do You Need Cyber-Fraud Insurance?

Two Part Test:

- 1) Do I Have a Computer?
- 2) Do I Have a Cellular Phone?



If You Answered “YES” to either, then you **NEED** Cyber-Fraud Insurance.

Investors Title
INNOVATIVE BY INSTINCT

53 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Who Are the Cyber -Criminals Today?

Who Are The Cyber-Criminals Today?

Hacker Type #1 – “Script Kiddies”

- Novice or “Wannabe Hacker”
- Maybe Mathew Broderick type character
- Someone who wants to be a hacker (or thinks they are) but lacks any serious technical expertise.
- They are usually only able to attack very weakly secured systems.
- There is enough “Low Hanging Fruit” to keep them in business

Investors Title
INNOVATIVE BY INSTINCT

54 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Who Are the Cyber -Criminals Today?

Who Are The Cyber-Criminals Today?

Hacker Type #2 – “Scammers”

- Your Email Inbox is probably full of their work.
- Discount Pharmaceuticals
- Time-Shares
- Personal Ads from Available Women in Foreign Lands
- Weight Loss Programs
- Viagra etc.
- Desire to Secure Your Representation

...sound familiar?

Investors Title
INNOVATIVE BY INSTINCT

55 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Who Are the Cyber -Criminals Today?

Who Are The Cyber-Criminals Today?

Hacker Type #3 – “Hacker Groups”

- Work anonymously
- Create tools for hacking.
- They often hack computers for no financial reason (e.g. for fun)
- Sometimes even hired by companies wanting to test their security.

Investors Title
INNOVATIVE BY INSTINCT

56 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Who Are the Cyber -Criminals Today?

Who Are The Cyber-Criminals Today?

Hacker Type #4 – “Political/Religious/Commercial Groups”

- Advancing a Political Agenda
- Not Interested in Money
- Many times Designed to Destroy
- Russians Accused of Hacking the Democratic National Committee just before convention
- New Form of Militant Terrorism

Investors Title
INNOVATIVE BY INSTINCT

57 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

Who Are the Cyber -Criminals Today?

Who Are The Cyber-Criminals Today?

Hacker Type #5 – “Advanced Persistent Threat Agents” - – (APT)

- A network attack
- An unauthorized person gains access to a network and stays there undetected for a long period of time.
- The intention of an APT attack is to steal data rather than to cause damage to the network or organization.
- APT attacks target organizations in sectors with high-value information, such as national defense, banks, and anyone with a lot of consumer data.

58 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Who Are The Cyber-Criminals Today?

Hacker Type #6 – “Phishers”

- An attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money)
- Often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Who Are The Cyber-Criminals Today?

Hacker Type #7 – “Insiders”

- Represent 20% of the Cyber-Fraud threat
- Responsible for 80% of the damage.
- These attackers are considered to be the highest risk.
- Often employees of the organization

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #1 – Casual Use of Passwords

- Should use complex passwords
- ALTA Best Practices Require
 - At least 8 characters
 - Uppercase and Lowercase
 - Letters and Numbers
 - Special Character
- Should change complex passwords regularly
(Every 3 Months Minimum)
- Should change factory installed passwords

Investors Title
INNOVATIVE BY INSTINCT

61 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #1 – Casual Use of Passwords

- Often Multi-Factor Verifications Are Used.

Question 1

What was your high school mascot?

What was your favorite pet's name?

What is your favorite movie?

What was your favorite teacher's name?

What is your favorite sports team?

What is your favorite meal?

What is your favorite ice cream flavor?

What is the first and last name of your first boyfriend or girlfriend?

Which phone number do you remember most from your childhood?

What was your favorite place to visit as a child?

Who is your favorite actor, musician, or artist?

Investors Title
INNOVATIVE BY INSTINCT

62

Question 3

Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #1 – Casual Use of Passwords



Spouse's Name	Employment
Kids' Names	Pets' Names
Parents' Names	Your Schools
Relationship	Kids' Schools
Favorite Food	Hospital Visits
Vacation Spots	Dentist & Doctor
Hometown	Access Stories
Your Birthdays	Life's Tragedies
Family Birthdays	& Rest of Your Life

63 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #2 – Casual Protection of Info That Should Be Secured

CONFIDENTIALITY NOTICE: This electronic mail transmission has been sent by a lawyer. It may contain information that is confidential, privileged, proprietary, or otherwise legally exempt from disclosure. If you are not the intended recipient, you are hereby notified that you are not authorized to read, print, retain, copy or disseminate this message, any part of it, or any attachments. If you have received this message in error, please delete this message and any attachments from your system without reading the content and notify the sender immediately of the inadvertent transmission at XXX-XXX-XXXX or me@lawfirm.com. There is no intent on the part of the sender to waive any privilege, including the attorney-client privilege, that may attach to this communication. Thank you for your cooperation.

64 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #3 – Inadequate Protections on Trust Accounts

- **ATLA Best Practice #2**
- Escrow Funds Held in Federally Insured Bank
- Escrow Accounts and Operating Accounts Separate
- Access Limited To Authorized Personnel Only
- Monthly Three Way Reconciliation of Escrow Accounts
- Separation of Duties
 - Separate Reconciliation From Disbursement Authority (*Required*)
 - Others - Writing Checks / Signing Checks (*Suggested*)
 - Initiating Wires / Approval of Wires (*Suggested*)
- Block ACH Access To Escrow Accounts
- Block International Access To Escrow Accounts
- Utilize Positive Pay or Reverse Positive Pay

Investors Title
INNOVATIVE BY INSTINCT

65 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #4 – Improper Disposal of NPI



66 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In! Access #4 – Improper Disposal of NPI



False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #4 – Improper Disposal of NPI

- Disposal and Decommission of Devices Containing NPI

- Computers
- Copiers
- Hard Drives
- Portable Media
- Phones



False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #5 – Internet of Things (aka IoT)

How Many Internet Connected Devices Do You Have

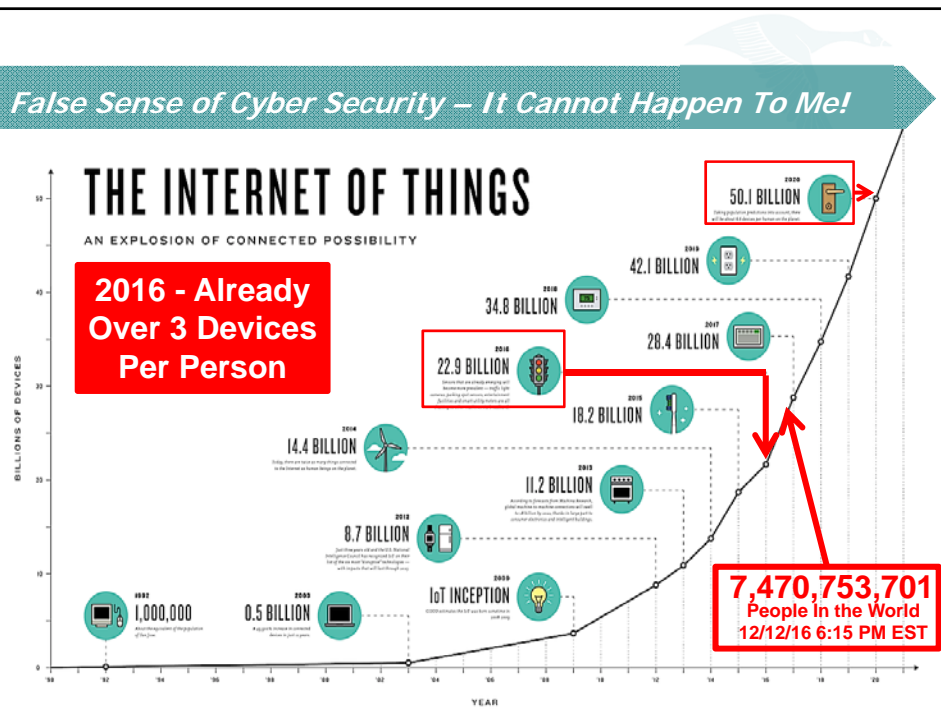
- Computers
- Copiers
- Television
- Cable Box
- Phone
- Smart Watch
- Refrigerator
- Coffee Maker
- Smart Home Lights
- Water Heater
- Garage Doors
- Dog Collar ETC.

How Many Internet Connected Devices Do You Have?

© Title
INSTITUTE

69 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education



False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #5 – Social Media

How Many Internet Accounts Devices Do You Have

- Facebook
- Google Plus
- YouTube
- Twitter
- Instagram
- SnapChat
- TeamSnap
- MySpace
- Skype
- LinkedIn
- Dating Sites
- Search Engines
- AOL
- Yahoo
- Ebay
- Marketplace Platforms
- Yelp
- IHaveNoLife.com ETC.

Investors Title
INNOVATIVE BY INSTINCT

71 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #5 – Social Media



Spouse's Name
Kids' Names
Parents' Names
Relationship
Favorite Food
Vacation Spots
Hometown
Your Birthday
Family Birthdays

Employment
Pets' Names
Your Schools
Kids' Schools
Hospital Visits
Dentist & Doctor
Access Stories
's Tragedies
& Rest of Your Life

REMEMBER THIS!

72 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #5 – We Hire Them And Give Them a Password



ors Title
BY INSTINCT

73 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot Happen To Me~~ Me!

Stories of Actual Breaches

Cyber-Fraud War Stories

***Personally, I'm always
ready to learn,
although I not always
like being taught.***

- Winston Churchill



© Mark Mullen

Investors Title
INNOVATIVE BY INSTINCT

74 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Cyber-Fraud War Stories

Experience is a hard teacher. The test is given first, the lesson afterwards

- Anonymous



War Stories

#1 Ransomware / Cryptolocker

- Computer or Network is compromised
- Computer Locked
- Data Encrypted

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
 Following violations were detected:
 Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
 This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200

Where I can buy MoneyPak? **Walmart** **Walgreens** **RITE AID** **K CVS** **7**
green dot **MoneyPak** **Walmart** **Walgreens** **RITE AID** **CVS** **7**

located on the back of your MoneyPak, in the payment area and press OK (if you have several codes, enter them one after the other and press OK).
 If an error occurs, send the codes to address fine@fbt.com.

77 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.
 Click <Next> to select the method of payment and the currency.

Private key will be destroyed on **9/24/2013 6:21 PM**

Time left
54 : 15 : 15

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

78 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

THE **FBI** FEDERAL BUREAU OF INVESTIGATION

IMAGINE YOUR PICTURE HERE

All activity of this computer has been recorded. If you use a webcam, videos and pictures were saved for identification. You can be clearly identified by resolving your IP address and the associated hostname.

You have been violating Copyright and related Rights Law (Video Music, Software) and illegally using or distributing content which infringe Article I, Section 8, Clause 8 also known as the Copyright of the Criminal Code of United States Of America

Article I, Section 8, Clause 8 of the Criminal Code provides a fine of two to five hundred minimal wages or a deprivation of liberty for two to twelve years.

You have been viewing or distributing prohibited Pornographic content (Child porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States Of America

Pursuant to the amendment to the Criminal Code of U.S.A. of May 28, 2011 this law infringement (if is not repeated - first time) may be considered as conditional in case you pay the fine to State.

Please note: Fines may only be paid within 48 hours after the infringement. As soon as 48 hours elapse, the possibility to pay the fine expires, and criminal case is initiated against you automatically within the next 72 hours!

Your Computer has been locked!

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$200. Payable through GreenDot

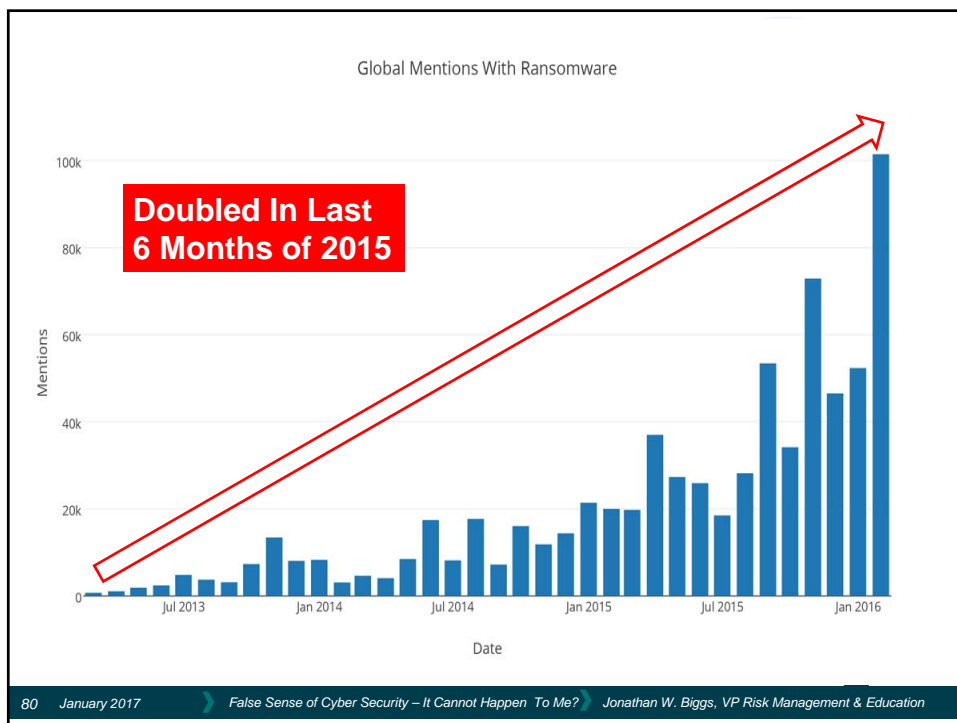
1 Take your cash to one of these retail locations:

Walmart CVS/pharmacy Kwik Fill

2 Pick up a MoneyPak and purchase it with cash at the register

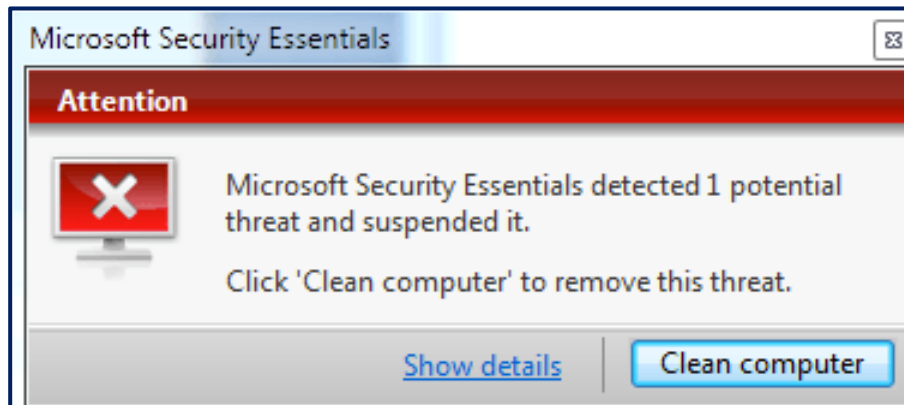
3 Come back and enter your MoneyPak code to unlock your Computer

79 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education



War Stories

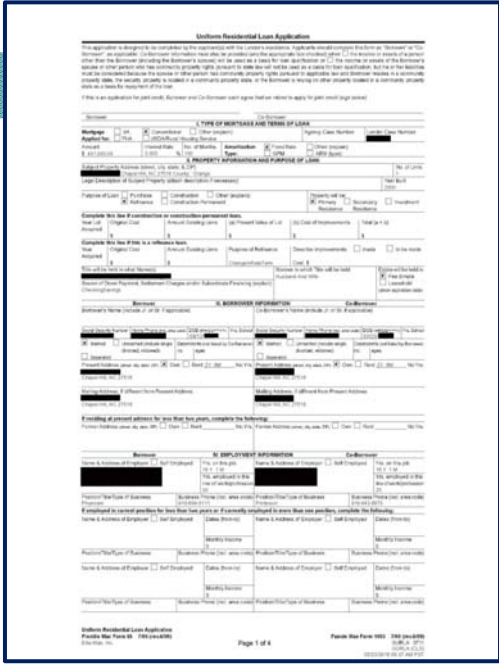
#2 Network Intrusions



War Stories

#3 Identity Theft

- Gain Access To Data Source, Computer or Network
- Steal More Than Account Numbers
- Steal Ability To Open Accounts
- Steal Ability To Verify Information at Banks, etc.
- Steal Ability To Verify Information at Retirement Accounts
- Steal Ability To Perpetrate a Crime in Your Name



~~Cannot~~ **DID** Happen To Me!

Universal Loan Application
Fannie Mae 1003
Freddie Mac 65

1. Deal Specific Information
2. Borrower Information
3. Employment Information
4. Income Information
5. Assets & Liabilities Info
6. Net Worth Information
7. (Total) Real Estate Info
8. Transaction Details
9. Borrower Declarations
10. Borrower Affirmation & Sigs
11. Additional Liabilities


83 January 2017
False Sense of Cyber Security – It Cannot Happen To Me?
Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#3 Account Hacked



84 January 2017
False Sense of Cyber Security – It Cannot Happen To Me?
Jonathan W. Biggs, VP Risk Management & Education

```

C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
  ://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
  Browsing)|https ://www.g[REDACTED]gmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
  Email from Google - Mozilla Firefox (Private Browsing)|accounts[REDACTED] Do Not Tell !
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts[REDACTED]gmail.com - Mozilla Firefox (Private Browsing)| Hello John
  [KeyName:Home] Dealer Room @wallstreettrade.com Confidential email: Hello,
  [REDACTED] John,[KeyName:Return][KeyName:Return] Please[REDACTED]use buy 1000 stock shares of our
  company.[KeyName:Return] Don't tell[REDACTED] anyone [REDACTED], because it will influence the sto
6 20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts[REDACTED]gmail.com - Mozilla Firefox (Private
  Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
  knowledge ; _0[REDACTED] [REDACTED] :- ) [KeyName:Return] Use my credit card number
  : [KeyName:Return] 1234 5678 9123 4567 [KeyName:Return] wich [REDACTED]
7 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts[REDACTED]gmail.com - Mozilla Firefox (Private Browsing)| [REDACTED]which
  expires 10/10.[KeyName:Return] The card security code on the back is :
  123.[KeyName:Return] [KeyName:Return] Thanks,[keyname:Return] Bob
8 20100326|1243|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
  Browsing)|www.playboy.com[KeyName:Return]
Nor 1848 chars 1866 bytes 10 lines Ln: 4 Col: 1 Sel: 0 (0 bytes) in 0 ranges Dos\Windows ANSI INS
85 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

```

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#4 Phishing Emails

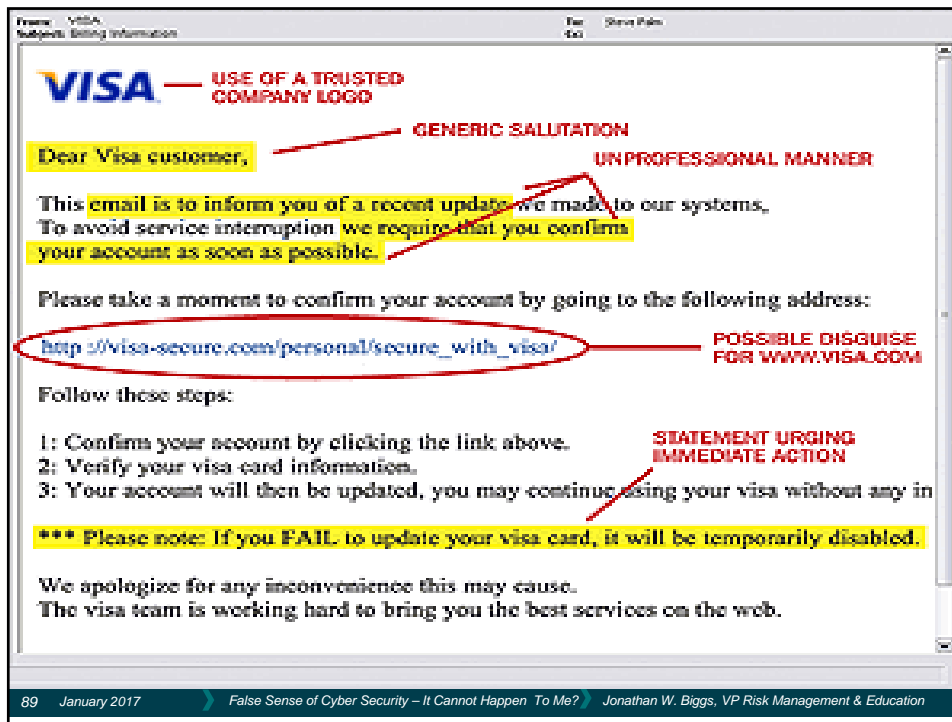
Pretending To Be From:

- Banks
- IRS
- Credit Card Companies
- Ebay.com
- Amazon.com
- Paypal.com
- Mortgage Companies
- Social Media (Such as Facebook)



Investors Title
INNOVATIVE BY INSTINCT

86 January 2017
False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education



False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing

- Fraudster tricks you into sending money to wrong place
- Frustrating & Infuriating
- Banks Tell You That They Sent Money Exactly Where You Told Them To Send It
- Will Not Put It Back
- Sellers' Proceeds
- Buyers' Funds
- Even Payoffs - Watch Out – Big Numbers

BIG AREA OF FRAUD RIGHT NOW

89 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing

From: Jason McClain <cliff.hward@mail.com>
Sent: Tuesday, March 15, 2016 9:04 AM
To: [REDACTED]
Subject: 403 Topaz Drive Morton, IL 61550

Good morning Angi,

← Sent directly to employee.

We need your assistance as regards to the above mentioned property, We need disbursement done as a wire transfer to a different bank, as we just got advised by my financial advisor. Inform us about this as soon as possible in order to send you bank details required for the wire.

Jason C McClain & Renee W McClain

Quick, short message and poor grammar.

91 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

From: Jason McClain [mailto:cliff.hward@mail.com]
Sent: Tuesday, March 15, 2016 10:34 AM
To: [REDACTED]
Subject: Re: RE: 403 Topaz Drive Morton, IL 61550

Thanks for getting back. We would like you to cancel the check as we out of town and won't be back for some weeks. Kindly cancel the check. How will you like us to send the wiring instructions to you? Here or Should we fax it..

Jason C McClain

Calls for a Change

Poor grammar and states they will be out of town for a long time.

92 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

From: Jason McClain <mc.jason@mail.com>
Sent: Tuesday, March 15, 2016 11:58 AM
To: [REDACTED]
Subject: Re: RE: 403 Topaz Drive Morton, IL 61550

Different e-mail
being used here.

How much is your international wiring fee ?

Wiring Instruction below.

Account name : MEIHUA Trade co. ltd (In beneficiary of Jason & Renee McClain) it a cooprate account
Account number: 582322418838
swift code: HSBCHKHKKH
Bank..HSBC BANK HONG KONG
Bank address...Queens road central , Hong kong

Out of Country

It's not common to
have a corporate
account with individual
beneficiary names.
Also misspelled
Corporate.

Looking forward to seeing the Wire confirmation slip

Thanks

Jason C McClain

93 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing



Investors Title
INNOVATIVE BY INSTINCT

94 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing

- Person or Person's Digitally Compromised
- Gain Information
- Information Used To Gain Confidence
- Confidence Used To Exploit Someone or Gain Advantage
 - Think Old Time Confidence Man
 - Think About Dating and Relationships
 - Think About Contract Negotiations
- Sometimes Confidence and Information Used To Steal
- Then It Becomes Criminal

Investors Title
INNOVATIVE BY INSTINCT

95 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

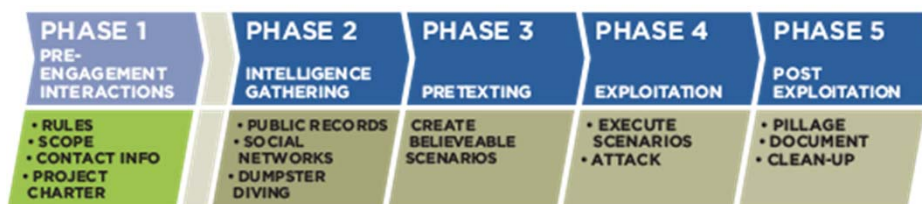
False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing

SOCIAL ENGINEERING



Investors Title
INNOVATIVE BY INSTINCT

96 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing



Spouse's Name	Employment
Kids' Names	Pets' Names
Parents' Names	Your Schools
Relationship	Kids' Schools
Favorite Food	Hospital Visits
Vacation Spots	Dentist & Doctor
Hometown	Success Stories
Your Birthdays	Life's Tragedies
Family Birthdays	& Rest of Your Life

REMEMBER THIS!

97 January 2017

False Sense of Cyber Security – It Cannot Happen To Me?

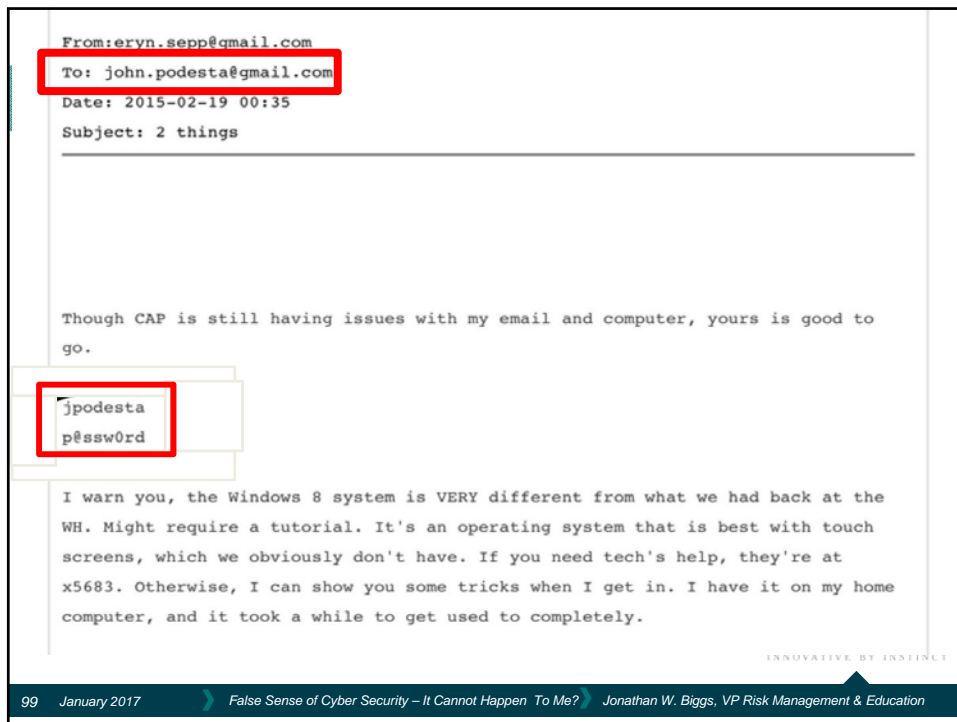
Jonathan W. Biggs, VP Risk Management & Education

```
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

98 January 2017

False Sense of Cyber Security – It Cannot Happen To Me?

Jonathan W. Biggs, VP Risk Management & Education



False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing

W. I. R. E. when you Wire

1. Proper Identification
2. Verbal Confirmation
3. Delivery Verification

What I Require Every Time

Investors Title
INNOVATIVE BY INSTINCT

100 January 2017 False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

WIRE. WHAT I REQUIRE EVERY TIME. Proper Identification. Verbal Confirmation. Delivery Verification.

File Number: _____ Closing Date: ____/____/____ Buyer(s): _____ Seller(s): _____

☐ INCOMING WIRE ☐ OUTGOING WIRE

STEP 1: PROPER IDENTIFICATION

Wire Instructions Sent to or Received from:

Contact Name _____

Party In Transaction
☐ Buyer ☐ Seller ☐ Lender ☐ Other _____

Verified Contact Phone _____

Encrypted Email _____

Fax Number _____

☐ Date Instructions Sent ____/____/____

☐ Date Instructions Received ____/____/____

Format of Delivery of Instructions
☐ Encrypted Email ☐ Fax
☐ Mail/Overnight ☐ Seller Docs/Affidavit
☐ Hand Delivery ☐ Other _____

Initials _____

STEP 2: VERBAL CONFIRMATION

Date Confirmation Call Made ____/____/____

*Call the Verified Contact Phone indicated in Step 1.
Do not rely on individuals that call you.*

Wire Amount: \$ _____

INCOMING WIRE
Which Trust Account: _____

OUTGOING WIRE

Account Name _____

Account Number _____

Routing Number _____

Bank _____

☐ Wiring Instructions Verbally Confirmed and Attached

Initials _____

STEP 3: DELIVERY VERIFICATION

Wire Authorized by (Of Outgoing Wire) _____

Wire Initiated by (Of Outgoing Wire) _____

Date Wire Sent ____/____/____ Date Wire Received ____/____/____

Date of Receipt of Wire Confirmation ____/____/____

Receipt of Wire Confirmed by _____

Type of Wire
☐ Loan Payoff ☐ Seller Proceeds
☐ Other _____
☐ Equity Line Payoff *Remember the Block & Close Letter*

Initials _____

CHANGE IN OUTGOING WIRING INSTRUCTIONS? CHANGES TO WIRING INSTRUCTIONS SHOULD REQUIRE A SECONDARY REVIEW

Change Requested by: _____ ☐ Buyer ☐ Seller ☐ Lender ☐ Other _____

Was Change Requested by Contact: ☐ Yes ☐ No Date Change Request: ____/____/____

Manner of Change Request: ☐ Encrypted Email ☐ Telephone ☐ Fax ☐ Other _____

Was Change Verified Independently through Steps 1 and 2? ☐ Yes ☐ No

Who Confirmed Change: _____ Date Change Confirmed: ____/____/____

Manner of Confirming Change: ☐ Verified Contact Phone (Recommended) ☐ Encrypted Email ☐ Other _____

Change Approved By: _____ Date Change Approved: ____/____/____

Investors Title
INNOVATIVE BY INSTINCT

800.326.4842 | www.invttitle.com/wire

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#6 Employee Theft

2015 Numbers

Employee Theft Statistics	Data
Amount stolen annually from U.S. businesses by employees	\$50,000,000,000
Percent of annual revenues lost to theft or fraud	7 %
Percent of employees who have stolen at least once from their employer	75 %
Percent of employees who have stolen at least twice from their employer	37.5 %
Percent of all business bankruptcies caused by employee theft	33 %

102 January 2017
False Sense of Cyber Security – It Cannot Happen To Me?
Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#6 Employee Theft

2015 Numbers

Amounts Stolen	Percent
\$1,000,000 and up	25.3 %
\$500,000 – \$999,999	9.6 %
\$100,000 – \$499,999	28.2 %
\$10,000 – \$49,999	16.8 %
\$1,000 – \$9,999	7 %
\$1,000 or less	1.9 %

**Median Amount
\$175,000**

Investors Title
INNOVATIVE BY INSTINCT

103 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!

Stories of Actual Breaches

War Stories

#6 Employee Theft

2015 Numbers

Demographics	
Men	59.1 %
Women	40.9 %
High School Degree	34 %
Some College	21 %
Bachelor's Degree	34 %
Postgraduate Degree	11 %

**26%
Discovered
By Employee
Tip**

Investors Title
INNOVATIVE BY INSTINCT

104 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Preventive Medicine Plan

C. Y. B. E. R.

Can

You

Be

Entirely

Ready ?

Investors Title
INNOVATIVE BY INSTINCT

Preventive Medicine Plan

1. Risk Assessment
2. Privacy Officer
3. Access Limited To Authorized Personnel Only
4. Physical Security of NPI
5. Digital and Electronic Security aka Network Security
6. Disposal and Decommissioning of NPI
7. Disaster Management Plan
8. Oversight of Service Provider Handling NPI
9. Notification of Security Breaches for NPI
10. Audit Procedures And Oversight of Information Security Program
11. Cyber-Fraud Insurance

Investors Title
INNOVATIVE BY INSTINCT

Preventive Medicine Plan

Element #1 – Risk Assessment

- a) Unauthorized access to NPI within the Company records
- b) Unauthorized request for access to the Company records
- c) Interception of data during transmission
- d) Loss of data in a natural disaster
- e) Corruption of data or systems
- f) Misplacement or loss of paper records containing NPI
- g) Compromise of NPI from disposal of records or equipment
- h) Unauthorized or unintended disclosure of electronic or printed NPI
- i) Failure to adequately monitor third party service providers and risks that third party providers could improperly use NPI

Investors Title
INNOVATIVE BY INSTINCT

Preventive Medicine Plan – Information Security

Element #2 – Privacy Officer

- Assess the Risks to NPI
- Assess Procedures for Monitoring Potential Threats To NPI
- Evaluate Procedures for and Methods of Detecting, Preventing and Responding to Identified Threats

Investors Title
INNOVATIVE BY INSTINCT

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #3 – Access Limited To Authorized Personnel

- Acknowledge Policy
- Criminal Background Checks (Going Back 5 Years)
 - Pre-Hire
 - Every 3 Years Post Hire
- Only Authorized Employees Access NPI
- Assign User Rights To Employee
- Terminate Employee Privileges Immediately Upon Separation

Investors Title
INNOVATIVE BY INSTINCT

109 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #4 – Physical Security of NPI

- Clean Desk Policy
- Privacy Policy
- Employee Access to NPI
- Physical/Location Security
- Removable Media

Investors Title
INNOVATIVE BY INSTINCT

110 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #5 – Digital & Electronic Security/Network Security

- Digital Security - Updated Systems, including OS security updates
- Backup Data - Performed Daily and Stored in a Secure Offsite Location.
- Internet Security - Antivirus, Anti- Malware, Firewalls Anti-Spyware
- Password Policy – Strong Passwords Changed At Least Every 3 Months
- Encrypted Email – Use it

Investors Title
INNOVATIVE BY INSTINCT

111 January 2017

False Sense of Cyber Security – It Cannot Happen To Me?

Jonathan W. Biggs, VP Risk Management & Education

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #6 – Disposal and Decommissioning of NPI

- Paper & Files Containing NPI
- Computers and Digital Devices Containing NPI

Investors Title
INNOVATIVE BY INSTINCT

112 January 2017

False Sense of Cyber Security – It Cannot Happen To Me?

Jonathan W. Biggs, VP Risk Management & Education

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #7 – Disaster Management Plan

- Create an Information Systems Disaster Recovery Plan
- Protect Against:
 - *Interruption To Business*
 - *Hardware Failures*
 - *Software Failures*
 - *Environmental Events*
 - *Theft*

Investors Title
INNOVATIVE BY INSTINCT

113 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #8 – Oversight of Service Provider Handling NPI

Types of Third Party Service Providers

- *Independent Searchers*
- *Couriers*
- *Janitorial Service*
- *Alarm Company*
- *HVAC, Plumbing, Electrical*
- *Off Site Storage*
- *IT Professionals*

Investors Title
INNOVATIVE BY INSTINCT

114 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

Preventive Medicine Plan – Information Security

Element #9 – Notification of Security Breaches for NPI

- All Employees and Third Party Service Providers Should Report Breaches of the Information Security Policy.
- If a Breach Occurs, Everyone Should Work with Affected Clients, Consumers, and Local Law Enforcement as appropriate.

Preventive Medicine Plan – Information Security

Element #10 – Audit Procedures And Oversight of Information Security Program

- Should Test Systems for Proper Operation
- Should Review Policies Annually For Potential New Threats and Security Measures
- Should Review Professional Best Practices for New Procedures and Protections
- Should Stay On Top of Information Security

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #11 – Cyber-Fraud Insurance

When All Else Fails; Have a Plan B – Cyber-Fraud Insurance

Investors Title
INNOVATIVE BY INSTINCT

117 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

*False Sense of Cyber Security – It ~~Cannot~~ **DID** Happen To Me!*

Cyber-Fraud Insurance

I TOLD YOU SO . . . Comes 2 Ways

- 1) When You Look In The Mirror After A Loss
- 2) When Your Insurance Agent Tells You, When He Gives You a Check

Either Way, I Told You So Is Coming.

Investors Title
INNOVATIVE BY INSTINCT

118 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

THANK YOU

Thank You

Investors Title
INNOVATIVE BY INSTINCT

119 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education

THANK YOU

Credits and Other Sites For Information

- <http://invtitle.com>
- <http://alta.org/bestpractices>
- <https://www.fbi.gov/investigate/cyber>
- <http://www.faronics.com/news/blog/7-types-of-cyber-criminals/>
- <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/>

Other than Investors Title Logos and Images, No Claim of Ownership is Made to Any of The Other Images Contained Herein

Investors Title
INNOVATIVE BY INSTINCT

120 January 2017

False Sense of Cyber Security – It Cannot Happen To Me? Jonathan W. Biggs, VP Risk Management & Education