MYTHS and MYTH BUSTERS

Myth 1 ▶	I am on top of cyber security and I have no worries.
Myth Buster ▶	**NO!** Cyber-criminals work 80 hours a week to avoid working 40 hours a week. In comparison to the cyber-criminals how many hours a week do you spend focusing on cyber-security?
What to do?! ▶	Thoroughly examine your business to assess the risks present. Develop and implement policies, procedures & protections to mitigate those risks and deter fraud.
Myth 2 ▶	Firewalls, Anti-Virus and Anti-Malware software are all the protection I need.
Myth Buster ▶	**NO!** Firewalls, Anti-Virus, Anti-Malware software are absolutely necessary, but it's human error that will allow most cyber-fraud to occur.
What to do?! ▶	Create a culture of fraud awareness. Develop and clearly document processes and procedures. Train and retrain your staff to follow these processes and procedures.
Myth 3 ▶	My employees are expertly trained in cyber-security; we do not need to do anything else.
Myth Buster ▶	**NO!** The most common form of cyber-breach or crime occurs because an excellent hardworking person is tricked into doing something incorrect. If an employee falls prey, it does not mean that he or she is a bad employee, but it does mean that they need to be aware of the ever evolving cyber-criminal scams.
What to do?! ▶	Provide ongoing training against cyber-crime and purchase cyber-fraud insurance to protect you when the unexpected happens.
Myth 4 ▶	I do not use the internet. I do not need to do any of this stuff.
Myth Buster ▶	**NO!** Private information or NPI can be released via telephone, fax, mail, even sticky notes! You need an information security plan if you have any communication in your business, regardless of the method.
What to do?! ▶	Develop and implement an information security plan that includes policies, processes and procedures for handling private information or NPI, regardless of the communication method.
Myth 5 ▶	I have done everything in this "Can You Be Entirely Ready?" brochure; therefore I do not need cyber-fraud insurance.
Myth Buster ▶	**NO!** People are still part of each of your processes, which means that mistakes can happen. If you use a computer or cell phone you need Cyber-Fraud insurance.
What to do?! ▶	Contact your Insurance Agent and discuss your coverage with everything in this brochure in mind.
Myth 6 ▶	My E&O insurance will cover me for cyber-fraud.
Myth Buster ▶	**NO!** General Liability and E&O Policies generally have exclusions for cyber-fraud.
What to do?! ▶	Ask your insurance agent about cyber-fraud coverage.
Myth 7 ▶	All cyber-fraud insurance is the same.
Myth Buster ▶	**NO!** Not all cyber-fraud Insurance is alike.
What to do?! ▶	Ask your insurance agent about Cyber Liability Insurance (loss of data) and Cyber Crime Insurance (loss of money). They are two distinct and different types of coverage.

National Investors
INNOVATIVE BY INSTINCT

3445 Executive Center Dr., Suite 110 | Austin, TX 78731
877.256.8098 | **nititle.com/wire**

C.Y.B.E.R.

Can You Be Entirely Ready?

National Investors
INNOVATIVE BY INSTINCT

Welcome to the 21st Century!

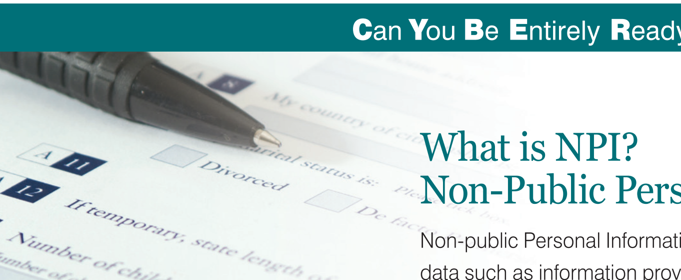
Today's technology puts the world at our fingertips. In seconds, and with the twitch of our thumb, we can get answers to our questions or send money around the world. Unfortunately, this 21st Century technology brings with it vulnerabilities that can allow Cyber-Criminals to threaten the security of our private information and money. We have a collective responsibility to protect ourselves from these new and emerging criminal threats. **YOU MUST PROTECT YOURSELF.**

	Stone Age	Middle Ages – 19th Century	20th Century	21st Century
Travel	Foot	Horse	Automobile	Hoverboard
Communication	Tablet & Chisel	Telegraph	Television	Internet
Money / Trade	Barter System	Coins & Paper Money	Check	Wire
Document Delivery	Hand Delivery	Stagecoach	Air-Mail	Email
Security	Hole / Cave	Iron Lock & Chain	Safe	Passwords
Criminals	Food Thief	Horse Thief	Organized Crime	Cyber Criminals

Some things change over time and some things never change. The fact that there are criminals amongst us will never change. However, how they perpetrate their crimes does and will continue to evolve. Therefore, how you protect yourself against their crimes should always adapt and change. You want to stay in the 21st Century. Do not let a Cyber-Criminal send you back to the Stone Age. Develop and implement an "Information Security Plan" to effectively protect your private information and money.

> "Three may keep a secret, if two of them are dead." – Benjamin Franklin

Can You Be Entirely Ready?



Some of the information you do not consider "secret" is valuable to cyber-criminals, like your birthday or your dog's name. This type of information can open the door to NPI.

What is NPI? Non-Public Personal Information

Non-public Personal Information definition: personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. NPI includes first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers.

> "Locks are made for honest people." – Walter A. Biggs

Steps to Consider for Your Information Security Plan

1. Perform a Risk Assessment
- Take an honest, deep look at every aspect of your business – the front door lock, your network security, your clientele, and your employees – to evaluate what risks are present that could stop you from doing business tomorrow. Plan to guard against those risks first. Consider:
  - – Where and how is information stored?
  - – Who has vs. who needs access to information?
  - – How is information communicated?
  - – Identify where you are vulnerable

2. Appoint a Privacy Officer
- Appoint a "Privacy Officer" who will be responsible for continually assessing your business for vulnerabilities and proposing and implementing changes in policy to protect against them

3. Limit Access to Information to Authorized Personnel
- Limit access to NPI to only those employees whose job function requires access
- Require that all employees sign and agree to adhere to your Information Security Plan
- Perform criminal background checks of all potential new-hires and of all existing employees at least every three years, and immediately terminate employee privileges upon separation

4. Implement a Wire Security Policy
- Please refer to National Investors informational materials entitled *"W.I.R.E. – What I Require Every time!"*

5. Implement Physical Security
- **Clean Desk Policy** – keep files closed during the day and locked away at night
- Computers should use **auto-locking screensavers**
- Adopt and maintain a **written privacy policy** which is communicated to all employees and clients
- **Secure all points of entry** (locks and key, electronic security system)
- **Password protect and encrypt** all removable media. Keep removable media in safe and secure location

6. Implement Digital and Electronic Security (aka "Network Security")
- Digital Security – updated systems, including OS security updates
- Encrypted Email – sending and receiving sensitive or confidential communications
- Backup Data – performed daily and stored in a secure offsite location
- Internet Security – Antivirus, Malware, Spyware and Firewalls
- Strong Password Policy – at least 8 characters including upper and lower case, numbers and special characters
  - – Assigned and limited to one per employee
  - – Passwords changed every three (3) months
  - – Reuse of passwords should be limited

7. Insure Proper Disposal and Decommissioning of NPI
- Shred or burn paper containing NPI
- Decommission digital equipment containing NPI (computers, hard drives, copiers, etc.)

8. Implement a Disaster Management Plan
- Protect yourself against business interruptions, hardware and software failures, catastrophic environmental events, and theft

9. Oversight of Service Provider Handling NPI
- Everyone should conduct due diligence on all third party service providers and ensure that they are either shielded from NPI or have appropriate safeguards for NPI to which they have access

10. Notification of Security Breaches for NPI
- In the event of breach, please refer to Investors Title informational materials entitled *"F.A.S.T. – Fast Action Stops Theft"*

11. Audit Procedures and Oversight of Information Security Plan
- Routinely test systems for proper operation
- Review policies (at least) annually for potential new threats and security measures
- Review professional best practices for new procedures and protections

Visit nititle.com for templates to help draft your Information Security Plan.

> "The only thing worse than training your employees and having them leave, is not training them and having them stay." – Henry Ford

Follow the Policies – Training Is the Key

All of the policies and procedures in the world will not protect your money or your NPI if you do not put the proper emphasis on the adherence to your polices. You provide this emphasis through complete, proper, and ongoing training to the policies. Follow the policies. Monitor those policies, as they will need to be updated as the cyber-threats continue to evolve. Train! Train! And train some more.