Cyber-Security:
Everyone's High Stakes War

White Paper

Provided by HUB International

The call came in the middle of the night to Ted and Karen's home. "Is Karen okay?" It was a good friend who had been on Facebook and saw Karen's plea for money - she was in London, her wallet had been stolen, and she was using Facebook to connect with friends who could wire her money to get home to the United States. But, Karen was right beside Ted in their house in Connecticut. She was not in London, and her wallet was in her purse. Karen's friend had almost become a victim of a modern cyber crime.

Cyber-Security: Everyone's High Stakes War

Cyber crime—an epidemic which is anchored in identity theft, but gone far beyond it—is everyone's problem.

Today, cyber criminals are becoming more sophisticated and searching for bigger payoffs. Vigilance in understanding the changing landscape and risks, while also constantly evaluating and re-evaluating your vulnerability, is critical to avoiding cyber-crime. Cyber criminals are working at a frenetic pace to reap the benefits of the information age. It is a high-stakes war no one can afford to lose.

"The 21st century intruder is well-prepared and well-equipped," says Paul Viollis, CEO of Risk Control Strategies (RCS), a New York City-based consulting and investigations firm that counsels the high net-worth community. "They no longer break into your house. They break into your life." According to Viollis, cyber criminals are increasingly targeting high net worth consumers and family offices because they represent a "one stop shop."[1]

It is imperative to understand the changing landscape of this type of crime. Identity theft is just the beginning. Cyber crime encompasses credit card fraud, hacking, "shoulder-surfing," fake Caller ID, "phishing," "spearing," and the next wave: medical identity theft.

Protecting assets is an ever-present reality in the information age. From the courtesy checks you receive from your credit card company to Gmail, Twitter, and Facebook, there is an abundance of fertile ground for financial crime. The good news is that there are a multitude of practical tips and safeguards everyone can implement to preserve their identity and property.

"Typically the first action a victim of identity theft takes is to install anti-virus software," said Tom Rusin, CEO of Affinion Security Center, a leading provider of identity theft protection and data breach resolution services. "Consumers need to be educated and prepared to proactively protect their identities in the online world, before it is too late."

According to *Information Week*, "Hacking isn't a kid's game anymore. It's big business. Online black markets are flush with stolen credit card data, driver's license numbers, and malware, the programs that let hackers exploit the security weaknesses of commercial software. Cyber criminals have become an organized bunch; they use peer-to-peer payment systems just like they are buying and selling on eBay, and they're not afraid to work together."[2]

Cyber Threats

A first step in protecting yourself is to be aware of the potential for crime. With the increase of online activity, the popularity of social networking, and our increasing comfort level with the Internet, criminals see opportunity and dollars signs. Gunter Ollmann, chief security strategist for IBM Security Systems, was quoted in a Georgia Tech Information Security Center Summit (GTISC) report about the evolving cyber crime economy, saying it is "an international conglomerate of professionally-trained authors motivated by high profit." This summit, one of the foremost in the security industry, publishes forward-looking information on cyber security threats each year. Following are the top five emerging cyber security threats for 2009: [3]

- Malware—software designed to infiltrate or damage a computer system without the owner's informed consent
- Botnets—groups of computers infected with malicious code and controlled by an outside master. GTISC estimated that botnet-affected machines could comprise as much as 15 percent of online computers

- Cyber warfare—the use of computers and the Internet in conducting warfare in cyberspace
- Threats to VoIP (voice communications over the Internet) and mobile devices
- The evolving cyber crime economy

Web 2.0, mobile convergence, and targeted messaging attacks were listed as last year's top emerging threats.

Cyber Criminal Industry

An entire industry of online "thieves" has been created. Today, there are three main categories:

- Low-level criminals who use kits (which can be bought, leased, subscribed, and pay-as-you-go) to create the specific malware required for their targeted crimes;
- Skilled developer and collectives of technical experts creating new components to embed within their commercial malware creation kits;
- Top-tier managed service providers that warp new services around malware kits to increase propagation and enable organized fraud on a global scale, feeding gains back into existing money-laundering chains.[4]

Understanding your Risks

Knowledge is power. In the information age it is imperative to stay informed about the types of cyber crime that you could fall victim to. There are a number of techniques that criminals employ to gain valuable information about individuals, which they then use to obtain passwords, Social Security numbers, and other vital information. Following are three categories of risk everyone should be aware of :

- "Spear Phishing" or "Whaling": These techniques target high net worth individuals and involve sending emails to money managers, financial advisors, and family offices. Often personally addressed, these emails include links that install malicious software.
- Fake Caller ID: Scammers use Internet-based phone service to fake the Caller IDs of banks and financial advisors. Because the phone ID bears the name of their bank or a trusted advisor, victims are tricked into providing personal information. Incoming calls, however, should always be suspect. Banks and related institutions rarely call to "verify account information."[5]
- Social Networking: The Internet and social media sites have made it far easier for both stalkers and scammers to learn about, and track, their intended victims. Chubb's Peter Spicer says "Twitter is a gift to stalkers if their intended victim is too open about who follows them and what they are willing to 'tweet' about." In addition, phishers have hijacked user accounts in order to send the user's friends instant messages pleading for emergency assistance – and money. Facebook warned its users earlier this year about the rise in phishing and spam attacks.[6]

> **"Your identity is a core asset."**
>
> ***~ Matthew Cullina, president, Identity Theft 911***

Five Types of Identity Theft

While not new, identity theft is evolving and it is typically the foundation for cyber crime. Five of the most common types of identity theft are:

- Department of Motor Vehicles—Use of a victim's identity to obtain a driver's license. Victims discover unpaid traffic tickets and DUI's under their name.
- Social Security—Use of a victim's Social Security number for employment purposes. These thieves also file taxes under a victim's name in order to obtain a refund.
- Criminal Identity—Use of a victim's information to escape fines or jail. Victims discover they have acquired a criminal record for bad checks, shoplifting, pornography, and prostitution among other crimes.

- Financial Identity— Use of a victim's information to obtain vehicles, real estate, and other goods or services.
- Medical Identity—Use of a victim's name, Social Security number, or insurance coverage to obtain prescriptions or medical services which reduces the victim's available benefits, damages credit, and makes it harder for victims to obtain an accurate copy of their medical records as they may be intermingled with those of the thief.

Matthew Cullina, CEO of Identity Theft 911, a firm that provides identity theft restoration services, says there are two non-credit risks that are often overlooked: estate identity theft, in which the personal information of a recently-deceased individual is used, and employment fraud, in which an individual uses another's personal information to obtain employment. He says the next trend may be a by-product of the recession: data breaches by disgruntled or laid-off employees.

Medical identity theft is the next wave in this type of crime. According to a 2007 report, the most recent source of federal data on medical identity theft collected by the Federal Trade Commission, more than 250,000 Americans fall victim to medical identity theft every year. Medical identity theft is the most difficult identity theft crime to fix after the fact, because victims have limited rights and recourses, according to the World Privacy Forum.[7]

The 21st century intruder is well prepared and well equipped…to break into your life according to Paul Viollis, CEO of Risk Control Strategies, a security firm in New York City.

Cullina also warns, "It takes a lot of resources and time to resolve a medical identity theft case. For one thing, there is no central source to alleviate the problem. With credit you have to primarily deal with three credit bureaus. With medical identity theft, it requires dealing with each medical provider to prove you are who you say you are. Less than 20 percent of medical records are electronic."

Medical identity theft is exacerbated by strict privacy laws, according to Cullina. The Health Insurance Portability and Accountability Act (HIPAA), enacted by Congress in 1996, set rules and limits on who can examine personal health information, which makes it difficult to correct. Cullina's bottom line: "Your identity is a core asset. Any damage to it will have serious consequences. So, manage it as you do your portfolio."[8]

For tips on preventing identity theft, refer to the checklist at the end of this paper.

Do you know...

what to do if identity theft occurs?

- **Report the fraud to the three major credit bureaus**
  Flag your accounts with "fraud alerts" requiring that you be notified whenever a request for a new account is received. Fraud departments for the three bureaus can be contacted at:

  Experian
  POB 9532
  Allen TX 75013
  888-397-3742

  Equifax
  POB 740241
  Atlanta GA 30374-0241
  800-525-6285

  TransUnion
  Fraud Victims Assistance Division
  POB 6790
  Fullerton CA 92634-6790
  800-680-7289

- **Notify credit card companies, utility service, telephone, and Internet providers that you have been a victim of fraud.**
- **Stop payment on outstanding checks and report the fraud to check verification companies:**

  National Check Fraud 843-571-2143

  Telecheck 800-710-9898

- **Close all accounts that have been compromised. Close and reopen checking and savings accounts.**
- **Notify the police**
  If the local police refuse to take a report, advise them that you need it for insurance purposes.
- **Contact your health insurance company, if you think your medical identity has been compromised. Your insurer's anti-fraud unit may be able to help.**
- **File a claim with your insurance provider**
- **File a claim with the Federal Trade Commission**
  Contact for the FTC is 877-ID THEFT

if you need a security firm?

High net worth individuals may wish to engage the services of a professional security consultant. However, selecting a consultant is challenging, given that there is no bona fide credentialing or accreditation process. A "certified" group of retired law enforcement officers may have an excellent background in investigations but may not be familiar with the risks facing high net worth individuals. The most prudent course of action is to seek referrals from trusted friends or colleagues and then perform rigorous due diligence.

In selecting a security firm, Viollis suggests these tips:

- Look for a firm that specializes in the high net-worth community. The firm needs to have knowledge of the culture and understand the concerns for privacy.
- The firm should have an established track record, verified credentials, and infrastructure.
- The firm must have adequate insurance.
- The firm should only rely on full-time employees, not part-timers or subcontractors.
- The firm should assign a representative to you who is available on a 24/7 basis.
- Find out if the firm's principals are the true decision makers or if there are silent partners who might represent a conflict of interest.
- Insist on an engagement letter in writing.

According to Chubb's Peter Spicer, the security firm should have some law enforcement experience. In the event of a crisis, they will know how to work with law enforcement agencies on the client's behalf. "There is an 'underworld' internet where criminals, predators and other bad actors lurk - exchanging information

and targeting people's identities, finances and at times, reputations," he said. A security firm without this expertise is missing a huge ability to "listen" to that underworld for relevant threats to its clients."[9]

Affinion Security Center's Tom Rusin adds that any form of protection needs to not only be able to help you resolve a theft, but also be able to identify one. "Ensuring that the Internet is being monitored for your personal information, both in terms of public facing websites and the underground, helps you to quickly detect when your identity is at risk." Rusin said, "Typically, the quicker you're able to react, the less financial harm is done."

how to insure cyber losses?

Insurers and brokers can take an active role in protecting the cyber security of their clients. A first step is educating the clients on the risks and putting in place coverage that indemnifies losses as broadly as possible, not just the expenses of restoring credit standing and identity, but where possible the actual financial losses. Many insurers offer identity theft restoration services, some of which are provided automatically at no charge and others that can be added to one's homeowners' insurance policy or as stand-alone policy.

There are many types of identity theft insurance available. Affinion's Rusin recommends finding a policy that protects a person's full financial assets. While the typical loss to a consumer who is victimized by identity theft is less than $1,000, financial institutions may not reimburse their customers for fraudulent cash transactions.[10] This makes affluent individuals with significant cash resources particularly vulnerable to financial loss when their identity is stolen.

When deciding on the level of coverage you need, ask if the policy offers the following:

- Assistance in obtaining emergency identity authentication and verification and access to their investment and bank accounts
- Assistance in replacing birth certificates, driver's licenses, passports and Social Security cards, checks and credit/debit cards
- Assistance in resolving credit and other problems in the event of identity theft or fraud, including a personal advocate to help the policyholder through the process of identity theft recovery such as the completion of a Federal Trade Commission affidavit
- Help in contacting police departments, creditors and credit rating agencies as well as assistance in creating a case file for insurance claims and law enforcement investigations
- Free credit and fraud monitoring
- Coverage for financial losses by third parties who gain access to checkbooks, credit cards, 401(k), savings accounts, or stocks and bonds
- Coverage for stalking victims if the stalker is known to the insured and subject to a court-issued restraining order.

Chubb, Fireman's Fund, and AIU Holdings (formerly AIG) which specialize in serving high net-worth individuals and families, are considering expanded coverage for actual financial losses.

how to lock out hackers and online thieves?

Treat your personal computers as you would your front door -- restrict access and know the key areas of vulnerability:

- Many security experts advise against using wireless networks. Hackers can stake out your home and "listen" to your online activity. Most if not all encrypted wireless networks can be broken into.
- Don't leave your laptop computer in hotel rooms or places where others can access it. Hackers install a keystroke tracker which then transmits your account names, PINs, and passwords to the receiving party, enabling them to access your online accounts.
- Be aware that free email services, such as Gmail, available from Google, have been criticized by privacy groups because many of these services come with a program that scans the content of

messages and sends users advertising based on words found in the email. Your deleted emails may also be stored on servers.

- When you log on to your bank account or any other password-protected site that stores your personal information, be sure to log off when you are finished and close your browser completely.
- Run the latest version of a proven anti-virus software program on your computer.
- Do not respond to pop-up ads that alert you to a virus infection. Legitimate anti-virus companies don't use pop-ads to inform you about the status of your computer.
- Use passwords that are not easily guessed. Do not share passwords with anyone.

how to protect your children?

Children are especially vulnerable to online crime. Warn your children of the dangers of the Internet including stalking, spyware, viruses and other potential threats. Other precautions include:

- Install an adult content blocking program, strong firewall, anti-virus/spyware software and monitoring to create the ability to review where your child has been and who/what is being e-mailed.
- Find out what computer safeguards are used by your child's school and in the homes of their friends.
- If your children use social networks, you should understand how they function and consider setting up their MySpace or Facebook accounts so you can monitor activity. Have frank and frequent discussions with your children about predators and so-called online "friends."
- Tell your children under no circumstances should they agree to accept gifts or meet anyone they've made contact with on the Internet. Instruct them to never give out identifying information such as their name, home address, school name, or telephone number.
- Experts agree that children should not be allowed to have a computer in their bedroom. Computers should always be in a common area of the home so parents can monitor use.
- When your children are preparing to go off to college, be sure to ask the university about the security of their network, especially if your child is going use the Internet to access a family bank account.

about other valuable resources...

- **Privacy Rights Clearinghouse.** More information, statistics and helpful tips *www.privacyrights.org*
- **Federal Trade Commission.** Tools to combat identity theft and information on how to file an FTC identity theft complaint. *www.ftc.gov*
- **Internet Crime Complaint Center (IC3).** Tips on preventing cyber crime, including identity theft, auction fraud, phishing/spoofing and dealing with spam. *www.ic3.gov*
- **Health Insurance Portability and Accountability Act (HIPAA).** information HIPPA, procedures and fees from insurers and providers. *http://www.cms.hhs.gov/hipaaGenInfo*
- **Medical Information Bureau (MIB Group).** If you have applied for individually underwritten life, health, disability income insurance in the past seven years, you can obtain a copy of your consumer file containing information on medical conditions and treatment annually at no charge. *www.mib.com*
- **My IDScore.** This free resource uses data analytics to find anomalies in how your personal information is used and provides you an identity score. The higher the score, the greater your risk of becoming a victim of identity theft. *www.myidscore.com*

Identity Theft and Cyber Security Checklist

Identity theft is a risk that continues to grow and change daily. Due to the many forms identity theft can take, including medical, credit, and financial theft, the threat remains prevalent and affects millions of people per year.

Keeping up-to-date with the latest prevention methods is the surest way to protect your assets and identity. Here are a number of steps you can take to reduce the risk of identity theft happening to you.

1. Reduce access to your personal information

If asked for your Social Security number, be sure to inquire why it is needed and how it will be protected.

- If you are applying for a credit card or insurance, you will typically be required to provide your Social Security number so the provider can pull your credit report.
- When asked for this information by your doctor's office, you should insist that the information on your insurance card is sufficient.
- Do not provide your Social Security number to online job websites or over the phone.

2. Eliminate unwanted credit solicitations

Reduce the chance of fraud perpetrated on you by removing unwanted solicitations. Take the following preventive steps:

- Contact 888-567-8688 and opt out of pre-screened credit card applications.
- Register for the National Do Not Call Registry that gives you a choice about whether to receive telemarketing calls at home. Go to https://www.donotcall.gov/register/reg.aspx, fill out the form and submit.
- Contact DMA Opt-Out Preference Service to limit direct marketing efforts: www.dmachoice.org.
- Ask your credit card companies to cease sending convenience checks.

3. Do not respond to emails requesting personal information.

"Phishing" is a technique used by criminals to solicit your personal data by sending what appears to be a legitimate email request from a recognized source, including banks, credit card companies or social networking sites.

- Be suspicious of any email that asks for sensitive personal information, even if the sender is familiar to you.
- Avoid filling out forms contained in an email message or pop-ups, even if it appears to be from a company that you do business with.
- If you receive an email from what appears to be your bank or credit card company, call them to confirm – and use the telephone number on your bank or credit card statement, NOT the one in the "phishing" email.
- Emails with misspellings or poor grammar are usually a good indication that the sender is a fraud.

4. Buy a shredder that cuts your paper into confetti

Thieves use discarded information to collect personal data on victims. A paper shredder reduces the potential for "dumpster diving" thieves to obtain your personal data from the following sources:

- Credit Applications
- Expired credit cards
- Old Bank and credit card statements
- Renewal forms that contain personal data
- Unwanted and unused convenience checks

5. Watch for "shoulder surfing" at ATM machines and gas pumps.

The ATM Industry Association reports over $1 billion in annual global losses from credit card fraud and electronic crime associated with ATMs.[10] Change locations if you are suspicious of the surroundings. If you notice unidentifiable transactions on your bank statement, notify your bank.

6. Keep Track of Insurance Cards

Guard your insurance card as you would your credit or ATM cards.

- Never give your medical information over the phone or lend your card to a friend.
- Medicare recipients need to be extremely careful as their Social Security numbers are printed on their Medicare cards.

7. Monitor your financial records

Review your credit card and bank statements each month. Refute any unauthorized charges within 30-60 days. Call your bank or credit card company immediately if you see any activity that could be fraudulent.

- Use passwords that are not easily guessed.
- Do not share passwords with anyone.
- Purchase virus, adware and firewall protection for your Internet access.
- If you have a wireless network, make certain that access is encrypted.
- Warn your children of the dangers of the Internet including stalking, spyware, viruses and other potential threats.

8. Monitor your medical statements

Every time you receive an explanation of benefits (EOB) form from your health insurance company, check it carefully.

- If you see charges for treatments you don't recall receiving, contact your insurance company for more information.
- Ask your insurer to provide you an annual summary of claims submitted under your name. Thieves may redirect your EOBs to a fake address, making it more difficult for you to identify a breach.

9. Monitor your medical records

Request a copy of your medical records from your physician(s) and keep in a secure place.

- If your medical identity is stolen and your medical records are altered, you'll have documentation to prove who you are when you report the fraud. It will also make it easier for you to prove the fraud and correct your medical records.

10. Review Social Security Benefits

- Review your Social Security statement to identify attempts to use your identity to seek employment.
- Contact 800-772-1213 to request earnings and benefit statement or request the information via the Internet at www.ssa.gov

11. Check your credit report regularly

- You can get a free annual copy of your report from all three credit reporting agencies at www.annualcreditreport.com.
- Experts recommend that you check your credit report at least every 90 days.

For more information, contact your HUB International Personal Insurance advisor.

Sources

1. Telephone interview with Paul Viollis, CEO Risk Strategies Consulting, 2009
2. "Information Week exposes the Internet Underworld," Bloggernews.net, February 12, 2007
3. "Emerging Cyber Threats Report for 2009," Georgia Tech Information Security Center
4. Ibid
5. "Cyber Scams on the Uptick in Downturn," *Wall Street Journal*, January 2009
6. "Beware of Facebook Scams," Aaron Broverman, Bankrate.com, March 25, 2009
7. "Medical Identity Theft: The Information Crime That Can Kill You," Pam Dixon, The World Privacy Forum, Spring 2006
8. Telephone interview with Matthew Cullina, Identity Theft 911, 2009
9. Telephone interview with Peter Spicer, Chubb Personal Insurance, 2009
10. "Identity Theft: The Aftermath 2008," Identity Theft Resource Center, May, 2009
11. "ATM Card Skimming on the Rise," Ike Wilson, *Frederick News Post*, May 27, 2009

HUB International thanks the following resources for their contribution to this white paper.

Affinion Security Center
Tom Rusin, CEO
203.956.8939
Trusin@affinion.com

AIU Holdings
Todd Triano, Vice President - Loss Prevention
908.679.3066
Cell: 908.399.0502

CHUBB
Peter D. Spicer, Communications Manager,
Chubb Personal Insurance
908.572.2843
pspicer@chubb.com

Fireman's Fund
Donald E. Soss, Chief Underwriting Officer
Personal Lines
415.899.2000

Risk Control Strategies
Paul Viollis, CEO
Scot Braunzell, Cyber Security
212.267.6992
www.riskcontrolstrategies.com

Insite Security, Inc.
Christopher Falkenberg, President
212.362.5700
cfalkenberg@insitesecurity.com

Identity Theft 911
Matthew Cullina, CEO
480.355.8500
mcullina@identity911.com

For more information about cyber security risks and insurance solutions, contact **James Kane**, president, HUB International Personal Insurance at james.kane@hubinternational.com, or your HUB International Personal Insurance advisor.

HUB International Limited
Headquartered in Chicago, HUB International is a leading North American insurance brokerage that provides a broad array of property and casualty, reinsurance, life and health, employee benefits, investment and risk management products and services through over 200 offices across the United States and Canada.

HUB Personal Insurance, Private Client Advisors
This dedicated practice within HUB International offers one of the largest and most sophisticated personal insurance practices in North America. Licensed on all 50 states and the territories and provinces of Canada, HUB International Personal Insurance has access to the products and services of hundreds of insurance carriers and intermediaries. For more information, contact personalinsurance@hubinternational.com

This information is provided for general information purposes only. It does not constitute professional advice and does not create a broker-client relationship. Please consult a HUB advisor about your specific needs before taking any action.