THIS PAPER IS PRESENTED BY:

FELTON, BERLIN & ERDMANN INSURANCE SERVICES, INC.
Robert H. Erdmann, ARM
(978) 548-3740
rerdmann@fbeins.com

CYBERSMART: UNDERSTANDING AND MANAGING CYBER THREATS TO HIGH NET WORTH INDIVIDUALS

pure INSURANCE | concentric advisors

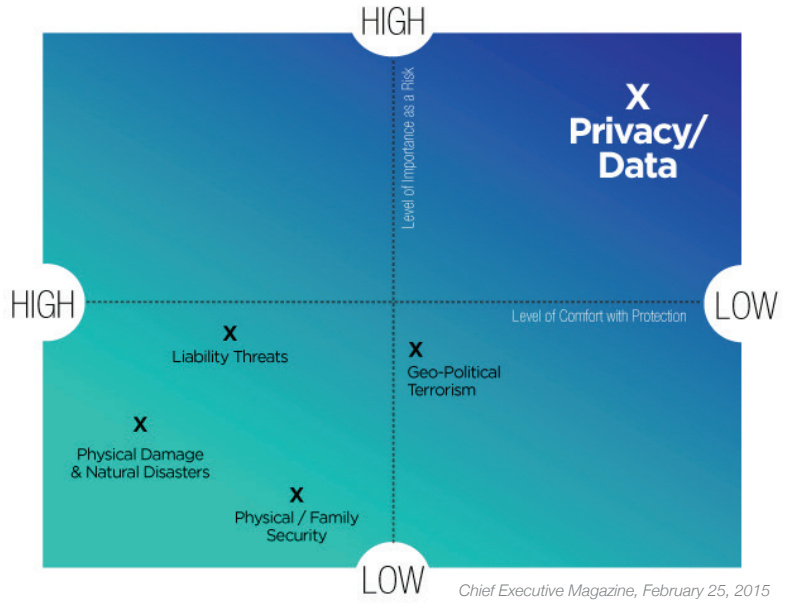
INTRODUCTION

Today, thanks to mobile broadband, children in developing countries have more data at their fingertips than the President of the United States had access to 30 years ago. It's estimated that by 2017, nearly 70% of the world's population will have mobile broadband subscriptions and by 2020, the number of networked devices will outnumber people six to one.[i]

While this evolution of the "information age" creates tremendous advantages and helps accelerate innovation, it brings with it new risks. Anthem, Home Depot, Neiman Marcus, Sony Pictures, JPMorgan Chase, Target and most recently, the U.S. Government, are just some of the household names who have had their customer and employee data exposed by hackers. These attacks have set industry and individuals on edge and have brought cyber crime into the mainstream.

While corporate attacks get most of the media attention, we must not forget that individuals—especially the high net worth—need to be vigilant about **cyber security**. The potential value of a high net worth victim to a cyber criminal and the uniquely complex lives of the high net worth, place them at higher risk of cyber crime. Trusted employees or third parties help care for their children, manage their finances, maintain their homes, automobiles and valuable collections, and more. Each of these connections creates potential for exposure and increases the **attack surface** for a cyber adversary to focus on. The trusted third party may not have malicious intent, but they may be the unknowing entryway into the individual's network or personal data.

The good news is that you can protect yourself against cyber risks. This paper touches on the key threats to the high net worth and provides advice to help reduce the associated risks. For additional information, visit our Cyber Knowledge Center at **puresituationroom.com/cyber.** PURE members may also call our cyber advice line at 855.573.PURE (7873) for more personalized assistance.



Chief Executive Magazine, February 25, 2015

A recent Personal Risk Index, produced in collaboration with *Chief Executive* magazine, revealed that the majority of CEO respondents view cyber risks as their greatest personal risk, rating it higher on their list of concerns than natural disasters and home invasions, among others. Further, of all the risks presented, respondents felt least comfortable with their ability to protect themselves and their families from cyber risks that threaten their privacy, data and wealth.[ii]

The number of fraudulent transactions and resulting loss of personal wealth is on the rise. In 2014...

47% of adults in the U.S. had personal info exposed by hackers

432M accounts were hacked as a result [iii]

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
An **attack surface** is the total sum of vulnerabilities in a given computing device or network that are accessible to a hacker.

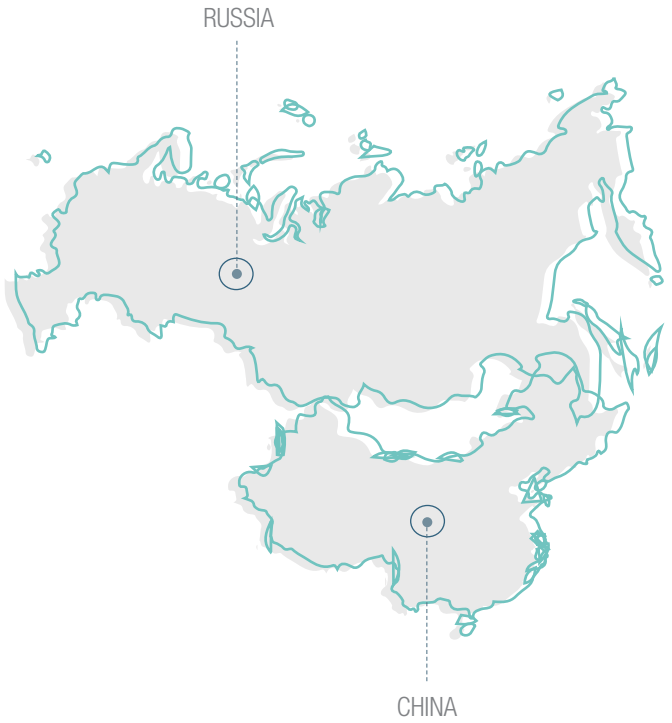
ORIGINS OF CYBER CRIME & THE UNDERGROUND ECONOMY

Cyber threat is as old as the internet itself. In its infancy, the internet was exploited by American hackers using a set of esoteric usernames such as Eric Bloodaxe, Phiber Optik, the Legions of Doom, and CypherPunks. While the names seemed playful, the acts of these hackers were not: overheating their target's electricity sockets to burn their houses down, breaking early banking infrastructure, and building powerful encryption systems to protect themselves.

In response to the emerging market for online illicit sexual content, Russian cyber adversaries created **bulletproof hosting** sites that could not be shut down or identified. As e-commerce took off, these sites pivoted into a platform for trafficking drugs and other illicit goods mainly to Western consumers. To drive traffic to these sites, spam email campaigns emerged. To make the infrastructure and delivery mechanism more efficient, hackers targeted individual computers around the world and created **botnets**. Botnets provided anonymity for organized crime, a discrete trade route via the computers of unsuspecting individuals, and automated deployment of spam, viruses, and other malicious processes.

Fast forward to 2015, a report issued by the Director of National Intelligence named cyber attacks as the principal national security threat facing our country—above terrorism, espionage and weapons of mass destruction.[iv] The report also named Russia and China as the leading threats to the U.S. due to their highly sophisticated cyber programs and weak cyber laws, which contribute to a breeding ground for cyber crime and allow cyber adversaries to freely carry out international cyber crimes without fear of retribution in these countries.[v]

While some attacks are politically motivated, the majority are carried out for financial gain. The potential profit to be made with someone's personal information, particularly if the individual is of high net worth, is great—in fact, it's a more lucrative industry than the illegal drug trade and the criminal has a lower risk of getting caught.[vi]



> THERE ARE TWO KINDS OF BIG COMPANIES IN THE U.S. THERE ARE THOSE WHO'VE BEEN HACKED BY THE CHINESE, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED BY THE CHINESE.[vii]
>
> FBI Director, James Comey

Bulletproof hosting refers to a hosting provider that will host virtually any content, from phishing sites to botnet command centers and browser exploit kits.
Botnets are networks of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages.

UNDERSTANDING THE MAJOR THREATS

The phrase "sophisticated cyber attack" has become commonplace, used to describe many high profile hacks and data breaches. The reality is that the majority of attacks—95 percent in fact—are not "sophisticated" at all.[viii] They do not rely on highly complex programming executed by "computer geniuses." Instead these attacks succeed simply because humans are not always as vigilant as they could be.

SOCIAL ENGINEERING

Social engineering is the act of obtaining personal information such as birth date, address, mother's maiden name, banking institution, or travel plans to aid in an attack against an individual. This tactic is used in a couple of ways: the social engineer can either manipulate individuals into giving up personal information about themselves or mine publicly available information, such as data that is available through social media profiles or online databases. High net worth individuals are often social engineering targets because they offer a greater payout potential.

EXAMPLE: The Dyre Wolf Campaign

A very bold and well-orchestrated example of social engineering is a scheme dubbed the Dyre Wolf Campaign, which targets organizations that conduct large wire transfers. It begins with a spam email containing a malware-laced attachment. Once installed on the user's local machine, the malware waits until the user navigates to their banking site. At this point a new screen appears explaining that the site is experiencing issues and that the user should call the number provided for assistance logging in. Upon calling, the hacker answers posing as the user's bank and dupes the user into providing their organization's banking credentials. This scheme has resulted in the theft of millions of dollars.[ix]

LARGE BANK ACCOUNTS ARE WORTH MORE ON THE DARKNET.

Illegal trading sites operate freely on the **Darknet**. It is here that stolen data is bought and sold for profit. These sites are alarmingly efficient; they include consumer reviews on the seller and details on the quality of their data. They offer discounts for buying in bulk and feature a user-friendly interface—much like an Amazon.com of the darknet. One such site, Rescator (which allegedly sold stolen information from Home Depot and Target shoppers) sells stolen personal information for a fee ranging from a few dollars up to the thousands.[x]

CREDIT CARD DETAILS	"FULLZ"	HIGH LIMIT BANK ACCOUNT
$9 - $13	**$30 - $40**	**up to $9,000**
	(Street slang for a package of all personal & financial records)	(Accounts with balances between $70,000 & $150,000)

These costs reflect the potential for return. Credit card information, for instance, allows the attacker to buy merchandise and sell it for $.50 to $.75 on the dollar. A "Fullz" would allow the attacker to steal the full identity of an individual giving them the ability to sign up for benefits, collect tax returns or apply for a loan. Details on high limit bank accounts fetch the highest price because they provide the greatest potential for return. When purchasing these details, the attacker expects to empty a large portion, if not all of, the account.

? The **Darknet** is a network with restricted-access websites commonly used for illegal activities.

UNDERSTANDING THE MAJOR THREATS, CONT'D

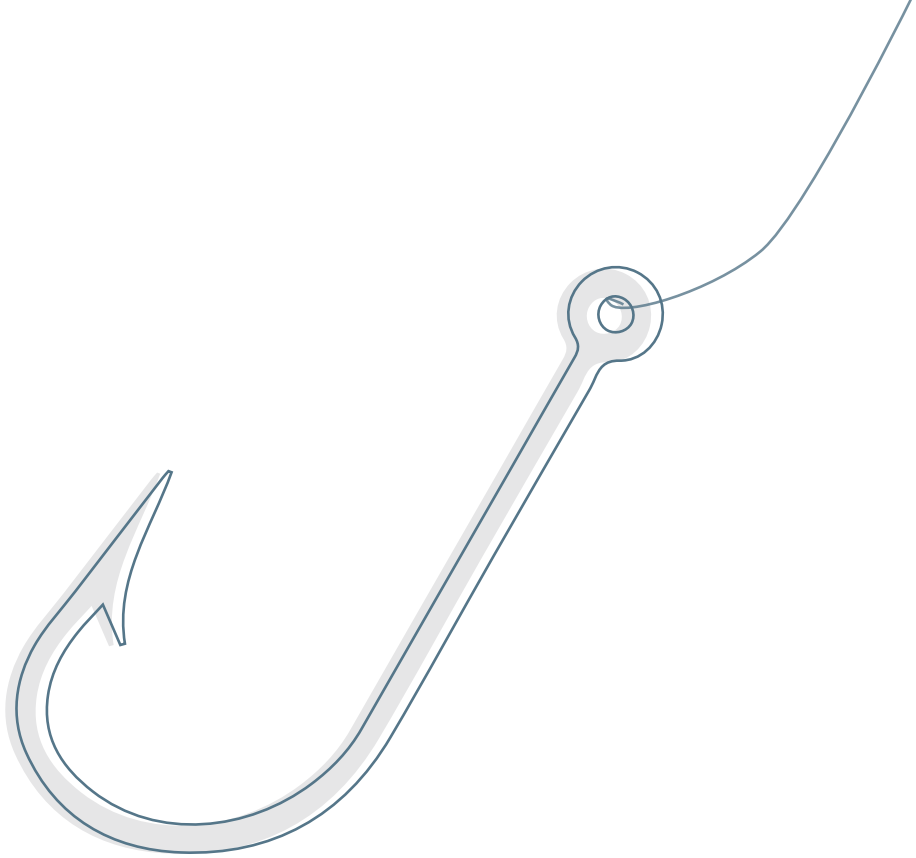
PHISHING

Phishing attacks, a form of social engineering, attempt to trick victims into revealing confidential information by posing as a legitimate website, email or caller. Cyber criminals play the odds through phishing attacks by sending out hundreds of thousands of emails with the expectation that a very small percentage will take the bait. Even a 1% success rate can be highly lucrative to cyber thieves.

Phishers often use tempting offers, such as giveaways, or piggyback on current, newsworthy topics to bait users. Most commonly, the targets are asked to open an email attachment; upon doing so, their computer becomes infected with malware, or they are redirected to a spoofed website where any information they enter could be captured.

While phishing is a broad stroke attack that tries to net as many victims at once, **spear phishing** focuses on a select few targets, often just a single, high net worth individual. A spear phishing email often contains personal details gathered through social engineering in order to appear legitimate, including names of business colleagues, friends and family. With a little effort, the criminal can piece together personal information about the target found through social media and other legal and/or illegal online sources creating a very believable email.

The compromising photos of celebrities stored on Apple's iCloud service were exposed not by attacking the technology, but by the attacker's ability to guess the celebrities' weak passwords. And it's not just celebrities who are at risk—executives in companies with more than 2,500 employees have a 1 in 2.3 chance of becoming the target of a spear phishing attack.[xi]



Phishing is a form of social engineering attempting to trick victims into revealing confidential information.
Spear phishing is a tactic that focuses on a select few targets, often just a single, high net worth individual.

UNDERSTANDING THE MAJOR THREATS, CONT'D

HOME NETWORK

While corporations are investing heavily to tighten their data security protocols, the security around most home networks falls short. As a result, hackers are turning their attention here. Of particular interest are the home networks of high net worth individuals, business owners, CEOs and other executives because of their access to valuable trade secrets, corporate financial information and simply because of their level of wealth.

A primary area of risk for your home network is your Wi-Fi. If not properly secured, you are susceptible to Man-in-the-Middle and Wi-Fi Spoofing attacks.

Man in the Middle: An attacker secretly sits between your computer and the websites you are accessing, capturing the communication of each party, and relaying it on, or possibly altering the communication.

Wi-Fi Spoofing: An attacker creates a Wi-Fi account that is named similarly to yours, attempting to trick you or your PC into connecting to it instead of your real, secured Wi-Fi account.

EXAMPLE: Another Unauthorized Transfer

A client of Concentric Advisors noticed a transfer of $25,000 from his account. Upon contacting the bank, he learned that the transfer was made by someone entering his correct username and password in the online banking system. He visited his local bank branch where he changed his login credentials. Once home, he logged in again from his computer. A short time later, another unauthorized transfer was made. Because his home Wi-Fi and router were not properly secured, the attacker was able to gain access to the connection and log all traffic and credentials being entered.

UNDERSTANDING THE MAJOR THREATS, CONT'D

PUBLIC NETWORKS

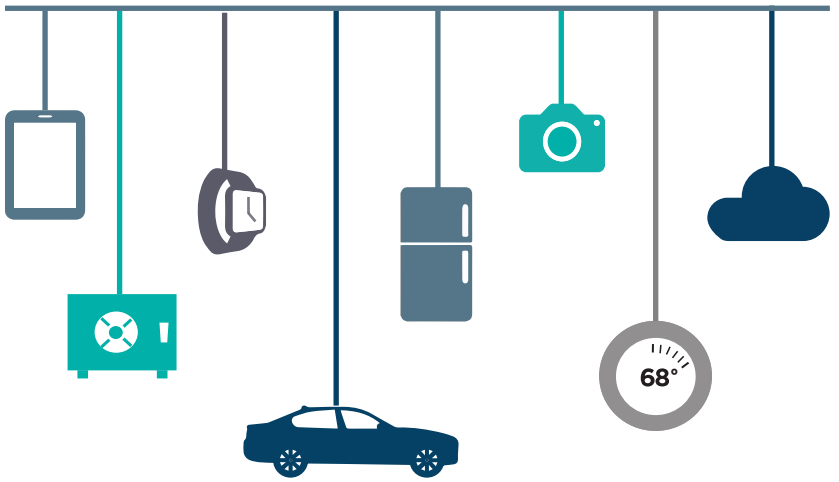
Public and open Wi-Fi hotspots (those that are available in hotels, cafes, airports, etc.) are inherently unsecure, even the ones that require a password to access. Hackers can easily infiltrate these networks and gain access to your activities and communications.

EXAMPLE: InnGate Router Exploit

Hackers are targeting hotel Wi-Fi networks to access high net worth individuals.[xii] Researchers have discovered a vulnerability in routers belonging to eight of the world's top ten hotel chains. At least 277 routers in 29 countries are believed to have been impacted. Of these, more than 100 were at locations in the U.S. Through the router, the attacker was able to install a very sophisticated keystroke logger on guests' computers. Despite the sophistication of the keystroke logger tool, this attack still relied on an unsuspecting individual clicking a phishing link (spoof Adobe pop-up and download prompt) to install the tool locally.[xiii]

THE INTERNET OF THINGS (IoT)

An evolving area of risk lies in physical objects we own that are connected to the internet. We rely on these devices to help automate our homes (creating 'smart homes') and our lives. Smart thermostats, webcams, network connected cars, even "wearables," among many other devices (collectively referred to as IoT), add a new layer of exposure. These now serve as another potential entry point by which an attacker can gain access to your network. This is a relatively new concept and the full scope of the risk is yet to be seen.



UNDERSTANDING THE MAJOR THREATS, CONT'D

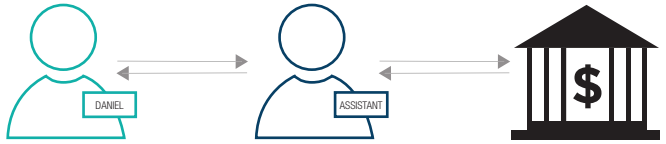
THIRD PARTIES: THE WEAKEST LINK

You are only as strong as your weakest link. For high net worth individuals, that could be an assistant or other employee, a financial advisor, accountant, wealth manager, or other trusted party—anyone with access to your systems, home, or assets. It also includes the companies or vendors you use in your daily life. Even though that third party may be trusted, it's important that you consider their risk management procedures in light of your own unique risk perspective.

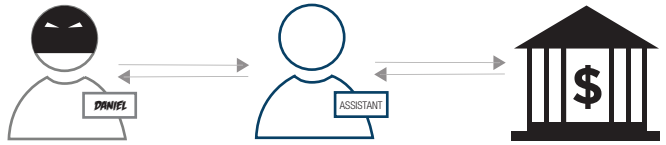
EXAMPLE: Posing as the Boss

When the personal assistant of a high net worth individual received an email request from her employer asking her to transfer $150,000 into the brokerage account of a familiar sounding third party, she assumed it was a legitimate request and processed it. When she received another email from her employer later that week asking for a second transfer of $90,000, she became suspicious. Although this email, like the one prior, was sent from her boss's personal email account and included his customary signature and private details of his personal account, something seemed off, prompting the personal assistant to pick up the phone. During this call she learned that neither request was actually from her employer. Unfortunately, the $150,000 was gone.

Normal Process:



Impersonation Scam:



THE IMPACT OF CYBER CRIME

FINANCIAL

Perhaps the greatest cyber risk that individuals face, especially the high net worth, is to their accounts held in financial institutions. While the Electronic Funds Transfer Act of 1978 provides some protection for consumers against credit card and debit card fraud, it does not contemplate all unauthorized or fraudulent bank transfers. Financial institutions each have their own policy on when and for what they will reimburse an account holder when funds are stolen. Unfortunately, this has all too often left the victim out of pocket for the entirety of the stolen amount.

INTELLECTUAL PROPERTY

The information that firms hold and exchange—including intellectual property, trade secrets and customer data—is of high value for adversaries like criminal syndicates, foreign governments, competitors, disgruntled insiders and hackers. Most corporations now invest heavily to prevent loss from cyber crimes, but it is important to remember that cyber thieves often target corporate/professional data through an employee's personal device or network. After all, most high net worth individuals access their "work" files and systems from home.

REPUTATIONAL

Reputational harm could have varied consequences such as a strained personal relationship if embarrassing photos or emails are released, to financial loss and reputational damage. The recent events that embroiled Sony following its hack, highlight what happens when proprietary or sensitive information is leaked to the public. Shortly after the apparent attack by the government of North Korea, one of Sony's co-chairmen stepped down.[xiv] It was reported that she was pursuing other opportunities, but it's likely her reputation was negatively impacted by the embarrassing and inappropriate emails that surfaced.[xv]

IDENTITY

The most common crimes committed with stolen identity are government benefits fraud, credit card fraud, and filing of false tax returns. For a high net worth individual with a more established credit profile, resolving the identity theft may be burdensome (though there are now firms who can work on your behalf to resolve the issue) but the impact on credit score and the ability to get new lines of credit is generally minimal.

PROTECTING YOURSELF

Managing your cyber security may seem overwhelming, but by understanding and implementing a few basic rules and strategies, you can successfully operate in a seemingly complicated environment. The following are just some of the strategies you can employ to help protect your data and your assets.

PRACTICE GOOD CYBER HYGIENE

PASSWORDS

The importance of good "password protocol" cannot be overstated. Passwords and login credentials are an important—and sometimes the only—layer in defending your information security, particularly when using online services or sites like cloud-based email, online banking, etc. While no password is completely undefeatable, the more complex the password is, the harder it is to crack.

Never use personal data as part of your password such as your birth date, social security number or mother's maiden name.

Avoid using actual words in passwords to decrease the chances of the password being guessed.

Use a password manager service, such as LastPass or 1Password, in conjunction with multifactor authentication, such as a tool like Yubikey, to create and keep track of strong and unique passwords. Be sure the password manager you select uses multifactor authentication (defined to the right) such as requiring a password and USB key.

Avoid password reset questions that anyone could answer by researching you or your family through paid or public services.

Always protect your mobile devices with a passcode. Adjust the settings on your devices so that they lock within a minute of being idle.

MULTIFACTOR AUTHENTICATION

This refers to the use of multiple points of authentication from independent categories to verify a user's identity. It typically combines:

"SOMETHING YOU KNOW"
(most commonly your username and password)

WITH

"SOMETHING YOU HAVE"
(e.g. your smartphone or device provided by bank)

or

"SOMETHING YOU ARE"
(e.g. your fingerprint)

When used together, these can greatly increase security since a hacker would need to complete multiple authentication requirements to access your account.

Multifactor authentication can be implemented on devices, in email, and in most banking, investing and social media websites. Visit puresituationroom.com/cyber for specific instructions on how to enable multifactor authentication on many of the most popular websites.

PROTECTING YOURSELF, CONT'D

REMOTE NETWORKING

Public Wi-Fi is notoriously unsecure. Instead, use a mobile or tethering hotspot, or a wireless router (such as **Mi-Fi**) that's been properly configured with WPA2 wireless encryption.

If you must use a public Wi-Fi, consider using a Virtual Private Network (VPN), such as Cloak. These tools add security and privacy to public networks.

EMAIL

Whether you use a paid email service (like Comcast) or a free one (like Gmail, Hotmail and Yahoo), the information you send through and store within your messages is not secure and is accessible by the service provider—some of whom (Gmail, for example) openly disclose that they mine and sell this information.

- **Never store sensitive information** (tax info, paystubs, SSN, checks, etc.) in your email.
- **Erase old messages** containing any bank account information and credit card numbers.
- **Never keep a saved document that serves as a master list of passwords.** For hackers, that's a treasure map.

If you must send sensitive information via email, be mindful of the fact that once you send it, you lose control over what the recipient does with it or what protocols they use to store or secure it. Consider an encryption tool and delete any messages once they are sent. Strong passwords and multifactor authentication are a must for email accounts.

SOCIAL PROFILE

The first step to securing your social profile is recognizing that certain information, if shared, can make you vulnerable.

- **Limit what you share.** Don't share information about your whereabouts when you're away from home and wait until you return to post photos or information. Similarly, don't provide too much personal information about yourself or your family, such as a home address and birth dates.
- **Limit who you share with.** Update the privacy settings so that the information you do post is only shared with a select group, rather than being publicly available.
- **Do not use geo-tagging** in any social media posts and do not advertise any time-place identifying information.
- **Be cautious when clicking.** Adversaries use several tactics to coerce people into clicking on malicious links, fake apps, plug-ins and enticing offers.

?

Mi-Fi's are small devices offered by cellular carriers that create a personal internet connection with a unique password.

PROTECTING YOURSELF, CONT'D

PROTECT YOUR HOME NETWORK

The security protocols in place for most home networks often pale in comparison to those enforced by corporations. To help secure your home network, consider the following points or contact a cyber security firm, such as Concentric Advisors, to help you and your family develop a safe and secure network.

ANTIVIRUS & FIREWALLS

All operating systems—within both PCs and Macs—are vulnerable to malware. Installing **antivirus software**, or manually scanning for viruses periodically with a standalone scanner, is an important layer of protection. However, no antivirus is guaranteed to stop all malware. Even paid services (e.g. Norton or McAfee) are not foolproof or necessarily better than the free antivirus software.

Firewalls are another important security layer in protection. Despite common misconceptions, firewalls are not a replacement for antivirus, but rather complementary, and should be enabled on your router and computer.

Firewalls sit on the edge of your network and block incoming connections from unauthorized users and software. Some can also block outgoing traffic—for example, if a virus on your computer attempts to "call back" to its commander for instructions.

THE CLOUD

While common cloud-based services (e.g. Dropbox, Google Drive and Box) are convenient and user friendly, they also present users with serious security exposures.

- **Avoid uploading medical, financial, or otherwise sensitive information to cloud-based services.** Although these services might encrypt your files in transit, they are not always encrypted at rest, and the service provider has complete access to them.

ROUTER & WI-FI

Take the following precautions to help secure your home network:

- **Change any default settings.** The default username and password of commonly available routers can easily be found online, allowing a hacker to gain access to your network simply by seeing the username on your Wi-Fi signal.
- **Encrypt your Wi-Fi.** Give your Wi-Fi network, identified by its SSID (a string of characters), a strong password so that, only those users you know and trust can connect to your network.
- **Look for spoofed Wi-Fi networks.** Before logging on, make certain that the network you are attempting to access is the correct network and not an imposter whose name closely matches that of your own network.
- **Turn off the UPnP feature.** Universal Plug and Play (UPnP), a setting on your router, is intended to simplify the process of adding new services to a network; however, it's also a common way for attackers to exploit your network.

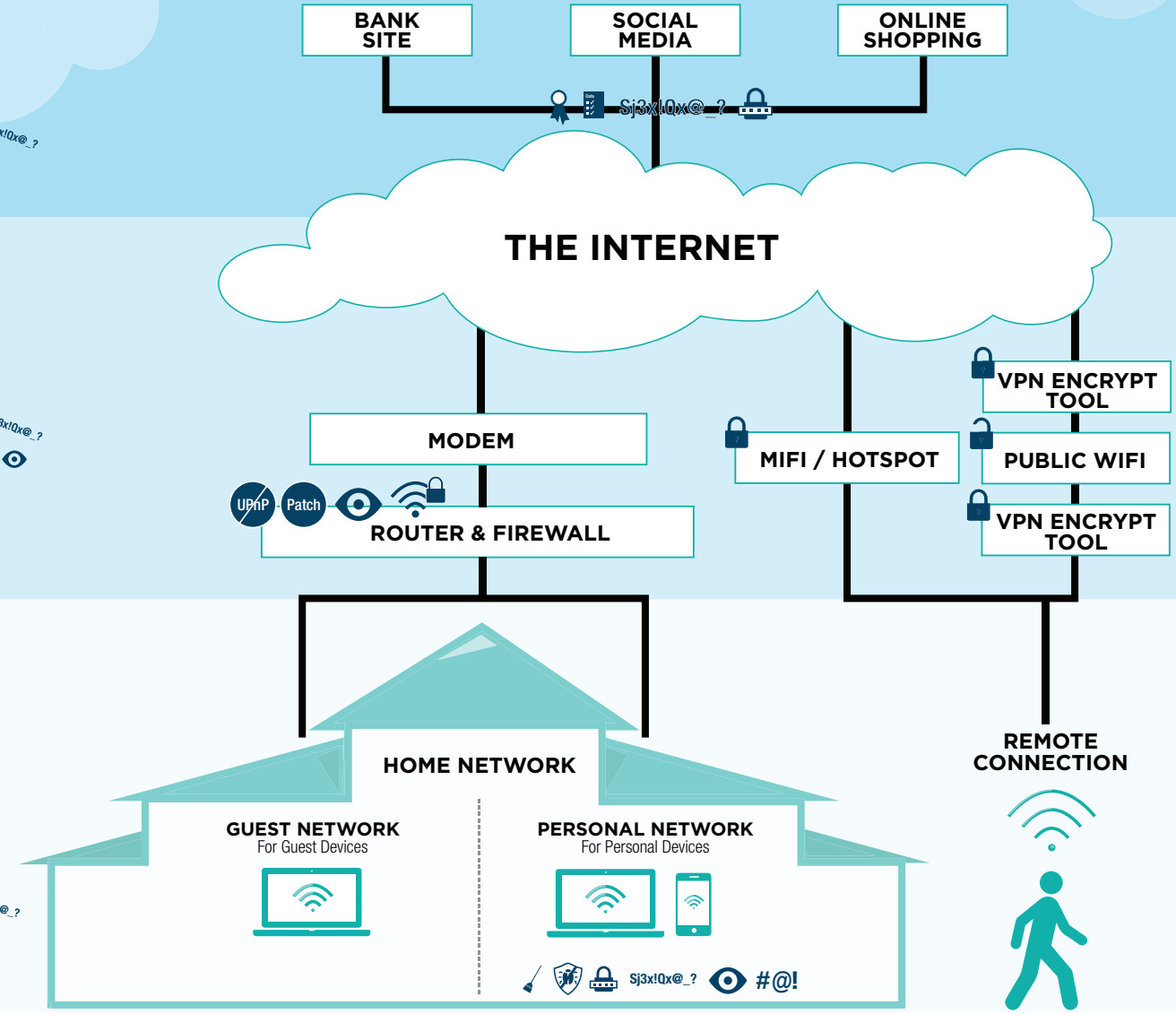
LAYERS OF PROTECTION

Good cyber security is about layers of protection. If every layer isn't protected, nothing is secure.

LAYER 3
Digital Certificates
Privacy Settings
Multifactor Authentication
Strong Passwords & Practices Sj3x!0x@_?

LAYER 2
Secure Router Settings
Secure Wi-fi (SSID; WPA2)
Strong Passwords & Practices Sj3x!0x@_?
Intrusion Detection Monitoring

LAYER 1
Multifactor Authentication
Antivirus
Network Scans
Segmented Network
SW Updates / Patches
Remote Wipe
Whole Disk Encryption #@!
Strong Passwords & Practices Sj3x!0x@_?



PROTECTING YOURSELF, CONT'D

BE THIRD PARTY-SMART

When it comes to dealing with your assets and financial information, the human element in the process must be considered. The protocol used and followed by your asset managers, assistants, attorneys, and others you have authorized to help manage your assets is just as important as the security of the technical systems they use. Make sure you have established protocols for dealing with money transfers:

Require oral confirmation and the use of a code word or phrase in order to process money transfers.

Set up a different, hard-to-identify email address used solely for your financial accounts.

Ask your financial institution what their policy is regarding stolen funds. All institutions have their own policies in place for this. If you are not satisfied with their response, consider another institution.

Request that additional layers of security (such as multifactor authentication) be required on your account prior to any transactions.

PROTECTING YOURSELF, CONT'D

EDUCATE & PROTECT YOUR CHILDREN

Even highly responsible children can compound cyber risk to the entire household. They are more trusting than adults. They inadvertently engage with cyber thieves in gaming situations. Some work around security to see sites their parents don't want them to visit. And, many of them are far ahead of their parents' ability to keep them from making mischief online—in fact, many of them act as the family's de facto tech support.

Discuss the following tactics with your children to help them protect themselves, your family, and your assets.

NEVER TALK TO STRANGERS, EVEN ONLINE.

Some people you meet online may not be who they say they are so it's best to avoid communicating with anyone you don't know. Tell an adult if a stranger tries to communicate with you.

AVOID ACCESSING PUBLIC WI-FI NETWORKS.

Even those that require a password are not secure. Similarly, be cautious of Wi-Fi spoofing on your home network.

DON'T SHARE PERSONALLY IDENTIFIABLE INFORMATION

Whether playing a game or using social media, never share any personally identifiable information.

- Use a nickname rather than your real name.
- Set your profile to private so that only your friends can see it.
- Avoid sharing personal information such as your full name, address, mobile number, school and photos. If information is required for something important ask a parent first.

NEVER GIVE OUT YOUR PASSWORD.

BE CAUTIOUS WHEN CLICKING

To avoid the possibility of inadvertently installing malware, be cautious of the links you click on when using social media. Adversaries use several tactics, including fake apps, plug-ins and enticing offers, to coerce people—especially children—into clicking on malicious links.

DON'T ACCEPT OFFERS THAT SOUND TOO GOOD TO BE TRUE.

They most likely are and you or your parents could end up with an unexpected bill or worse. When in doubt, ask a parent.

DON'T COMMIT OR TOLERATE CYBER BULLYING.

Tell a parent if you see it.

USE CAUTION WHEN DOWNLOADING FILES.

Peer-to-peer (P2P) file sharing sites allow users to easily share photos, videos, and other content. However, if the wrong file is downloaded, your device/network could become compromised.

ADDITIONAL PRECAUTIONS PARENTS CAN TAKE:

Install parental control software. Both Windows and Mac offer free options and there are other paid options available through third parties, such as Net Nanny®.

Set up unique profiles. If your children use a shared device, set up a separate user account for them with limited permissions and higher security settings.

Review your kids' social media profiles. It never hurts to check-in to ensure they are not at risk.

IMPROVE YOUR "CYBER STREET SMARTS"

Now that you're more familiar with some of the threats across the cyber landscape and can put some protection strategies in place, assess the services and companies you transact with to identify whether or not that relationship puts your personal data at risk.

Consider the online asset management tools you rely on to help seamlessly and conveniently manage your finances (e.g. Yodlee, Wealth Access) and your collections (e.g. Collector Systems, Vinfolio). In working with services like these, you entrust a great deal of personal and financial information to them—information that could leave your wealth exposed if it were to fall into the wrong hands. Beyond using your data for the intended service, what do they do with it and how do they ensure it's protected? What about the other sites that you transact with?

To better protect yourself, vet the security and data management protocols of the online vendors you interact with before sharing any personal or financial information. To help in this process, consider the following:

VENDOR-VETTING CHEAT SHEET:

1. What is the company's policy on selling or sharing customer data? If they do sell or share it, can you opt out? Know the company's policy on selling or sharing data.
2. Once they have your data, who owns it, you or the company? Will the company allow you to keep your data if you move on? And if you do move on, discuss whether or not the company retains or deletes your data.
3. Identify which individuals have digital access to your data. (e.g. Everyone in the company? A handful of administrators? Customer service reps?) Is a background check done on these individuals?
4. See if the company will submit to a NDA/Confidentiality and Use agreement that you send to them.
5. Understand the credentials or access controls that are in place to limit when people can access your data and how. (e.g. You have a home office and only want certain people in the office to have access.)
6. Ask if there is an automatic/system-generated log each time your data is accessed (saying who accessed, when, and what was done).
7. Make sure your login username/password is encrypted during transmission (e.g. Https/SSL).
8. Ask if there is multifactor authentication available for login.

HOW WE CAN HELP: PURE CYBERSAFE SOLUTIONS℠

Helping PURE members to live more confidently in a world of increasing cyber exposure and risk.

PURE CyberSafe Solutions was designed to help you assess, prevent, detect and respond to cyber threats. These solutions include:

Resources and Services to Help You Prevent Loss

Cyber Knowledge Center

Information is power, so we've created a Knowledge Center to help you better understand cyber threats and learn how to mitigate risks. Among other things, the Knowledge Center includes valuable content and an interactive diagnostic tool to help you assess your vulnerability to cyber risks. Visit puresituationroom.com/cyber.

Cyber Advice Line

Cyber Risk specialists are available to assist you with specific questions or concerns regarding the prevention, detection and response to cyber attacks. Call 855.573.PURE (7873) between 9AM – 8PM EST Monday through Friday for assistance.

CyberSafe Fundamentals Check

As part of our in-home PURE360™ Risk Management Consultation, PURE Risk Managers will conduct a 10-point cyber risk assessment designed to help you identify and mitigate major vulnerabilities in your home network, devices and online activities.

World-Class Services Provided by Concentric Advisors™

PURE has partnered with Concentric Advisors, innovators in the field of personal security, to bring you custom fee-based solutions designed to address evolving cyber threats and their associated risks.

Home Cyber Security Audit: An audit of your home network, devices, security protocols and usage designed to identify and help manage vulnerabilities.

Social Engineering Assessment: An analysis of the publicly-available personal information that exists online about you. Through this assessment, Concentric will identify vulnerabilities by predicting how this information can be used against you, and make practical recommendations to help mitigate these threats.

CyberShield: A managed monitoring solution designed to detect and respond to intrusion attempts on your home network. Through 24/7 automated monitoring and human data analysis, Concentric can identify and respond to threats, as well as identify emerging threats or related trends.

Valuable Coverage and Restoration Assistance

PURE's High Value Homeowners Policy provides coverage for:

Liability. For claims and lawsuits brought against you as a result of cyber-related property damage or personal injury, we will pay the defense costs and damages, up to the liability limit on the policy. For example, if your child is accused of committing cyber-bullying, or a hacker—using your social profile—posts slanderous comments, or exposes your personal correspondence that is damaging to a third party.

Identity Theft Restoration. Following an identity theft incident, we will pay the full cost for an identity restoration consultant to restore your credit record and personal identity.

Financial Loss. In the event of unauthorized use of your credit card or unauthorized electronic transfer from your bank or other asset account, we will pay up to $10,000.

Additional Service

Through one of our preferred *identity theft protection* providers, you can obtain monitoring and restoration services at a discounted rate.

Monitors your credit report, SSN and black market websites and alerts you of any suspicious activity with your data.

Manages the restoration process by eliminating the hassles associated with canceling and replacing credit cards, driver's licenses, Social Security cards, insurance cards and more.

To learn more about PURE CyberSafe Solutions, visit pureinsurance.com/cyber or call 888.813.PURE (7873).

ABOUT PURE

Privilege Underwriters Reciprocal Exchange (PURE) is a member-owned insurer for responsible families with homes insured for $1 million or more. Designed from the ground up in 2006, PURE has grown by more than 40% each year since inception by providing what is widely considered to be the best service experience in the industry—helping our membership feel smarter, safer and more resilient as they enjoy their success. We offer best-in-class, customizable coverage throughout the U.S. for high-value homes, automobiles, jewelry, art & other collections, personal liability, watercraft and flood. Inspired by some of the finest policyholder-owned companies in the world, PURE emphasizes alignment of interests and transparency. Thanks to a low cost of capital, careful member selection, and proactive risk management, PURE members report average annual savings of more than 25%*. Visit **pureinsurance.com** for more information.

ABOUT CONCENTRIC

Concentric Advisors is a security company specializing in sophisticated cyber, physical, and personal security for private individuals, their families, and businesses. Concentric believes all security should have a focus on constant innovation which is essential for staying ahead of evolving threats.

Our clients include some of the world's largest companies, most recognized brands, and most influential people in the technology, finance, philanthropic and industrial sectors. Using our network of government-level resources, we manage complex global operations across 46 countries and offer a broad range of services from cyber security, residential security, personal protection, and ongoing risk analysis. Our ultimate goal is to provide smart, customized security and risk mitigation services to enable our clients to maintain their privacy and position as industry leaders.

Our in-house team of industry professionals boasts unique qualifications and unmatched expertise. Their impressive record spans British and U.S intelligence agencies including the most renowned and elite positions in Scotland Yard's Special Branch, British Special Boat Service (SBS), the U.S Foreign Service, U.S. Secret Service and law enforcement. Concentric expertise is regularly sought to advise governments and international agencies. Visit **concentricadvisors.com** for more information.

ABOUT FELTON, BERLIN & ERDMANN INSURANCE SERVICES, INC.

At Felton, Berlin & Erdmann we specialize in providing high net worth individuals and their families the highest level of risk management services in the nation. In today's complex and litigious environment, having the right personal insurance program is paramount in protecting your families' assets, wealth and reputation. Our staff of experts consult with each client and create a customized personal insurance solution based on the unique needs of affluent individuals. With an average staff tenure of over fifteen years, you can rest assured that our team of advisors will provide you with the dedicated, knowledgeable and superior service that you expect and deserve. You've worked hard for your lifestyle, let us help you protect it. Visit **fbeins.com** for more information.

ENDNOTES

[i] Comprehensive Study on Cybercrime (2013) published by United Nations Office On Drugs And Crime: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[ii] http://chiefexecutive.net/2015/02/25/privacydata-security-remains-the-no-1-personal-risk-concerning-mid-market-ceos/

[iii] http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

[iv] http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf]

[v] Concentric Advisors

[vi] http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

[vii] http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10

[viii] http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=45352708151714315308358&cm_mc_sid_50200000=1431550991

[ix] http://securityintelligence.com/dyre-wolf/#.VVotRLlViko

[x] http://passcode.csmonitor.com/identity-trade

[xi] https://www.symantec-wss.com/campaigns/15948/assets/Symantec_WSTR_PT2_UK.pdf]

[xii] http://abcnews.go.com/Technology/cyber-crime-gang-targets-travelling-executives-hotel-wi/story?id=26806725

[xiii] http://www.wired.com/2015/03/big-vulnerability-hotel-wi-fi-router-puts-guests-risk/

[xiv] http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[xv] http://www.bloomberg.com/news/articles/2015-02-05/sony-s-pascal-to-step-down-as-studio-co-chairman-for-new-role