Accomplishing Risk-Based Decisions

CyberSecurity Risk Environment – 2013

Dave Hall
ESEP/CISSP
Hall Associates
301 641-1530
halld105048@yahoo.com
http://www.linkedin.com/pub/dave-hall/22/4b6/5a2

Why Do I Care About Cybersecurity?

Businesses and individuals increasingly work with and through the Internet and computers, making the risks inherent in these systems far more threatening than ever. **You are increasingly "connected"**.

There are more and more complex threats "in the wild", making Internet and IT security harder to accomplish. It's not a case of **IF**, but of **WHEN**. **NO** system or device can be made absolutely secure.

Internet and IT risks, when they occur, will cause business and individual losses - lost resources, lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity - lost money, lost identity, lost credit, lost reputation.

And if you don't know what risks/threats you face, you will not be prepared for them.

What is Cybersecurity Risk?

Cybersecurity risk definition: Any threat to your ***personal or business information***, ***critical systems/devices*** and ***business processes***.

Why me? Business management and personnel have a responsibility to identify areas of risk and respond in a timely fashion to these by improving processes, augmenting controls and requiring testing to ensure that the business ***is properly identifying and responding to risks***. Individuals also have a responsibility to ***properly identify and respond to risks*** to maintain what they and their family has.

Why do I care? Failure to identify, assess, control and monitor risk sets both businesses and individuals up for serious security breaches and financial losses now and down the road.

What is the main issue? The challenge for most businesses and individuals is to determine what risks pertain to them and to identify a repeatable process to identify, assess, control and monitor risk ***without interrupting their business or personal activities.***

Cybersecurity from a Systems Engineering Viewpoint

System Definition

A system is a set of interacting or interdependent components forming an integrated whole

Country
(System)

State
(Subsystem)

Community
(Unit)

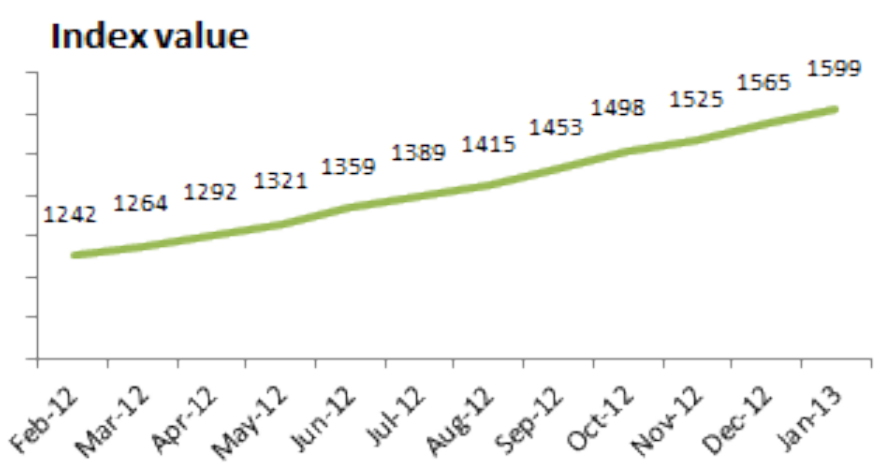
Group/Company
(Boards)

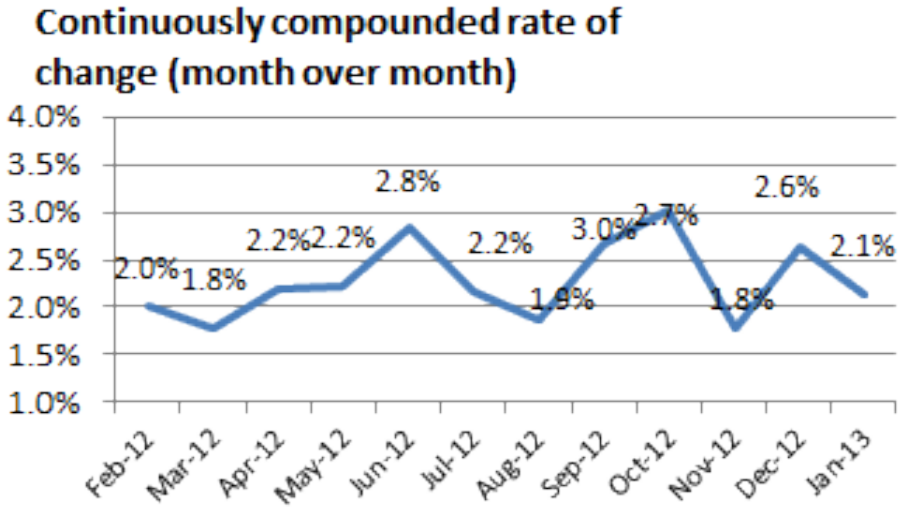
The Boeing Company, ADTRAN, SAIC, University of Alabama in Huntsville, Teledyne Brown Engineering, Benchmark Electronics, Inc., Northrop Grumman, Direct TV, West Corporation, COLSA Corporation, CSC, Redstone Federal Credit Union, ITT, Lockheed Martin, Dynetics, Raytheon Company, Yulista, City of Huntsville, Churches, Professional Groups

Individuals
(Components)

Cybersecurity Index

The Index of Cyber Security is a measure of risk. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite.





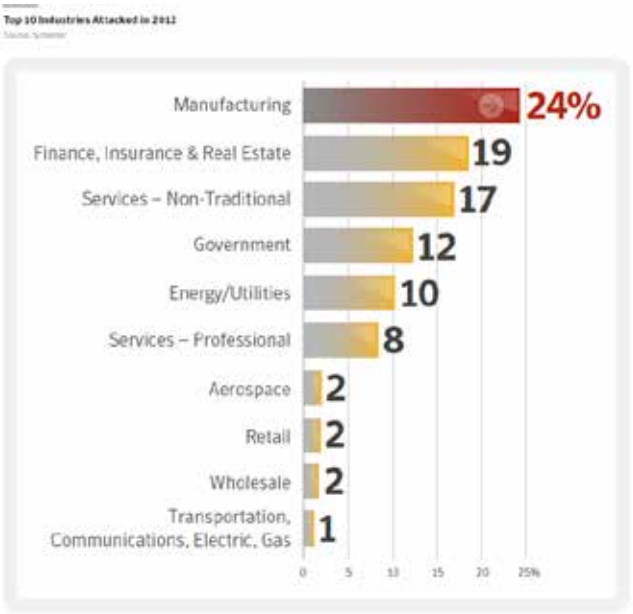
The top sub-indices for the Index did not change, neither did their relative positions.

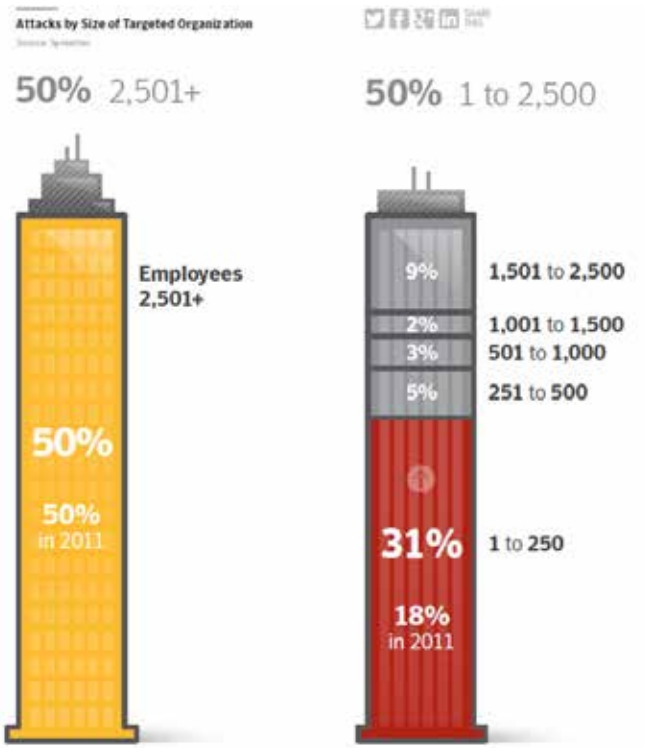
- Risk from counterparties, ie the risk from information compromise as a result of sharing information with insecure third parties (counterparties, vendors, partners etc), was rated as the top risk by our respondents.
- The activist-hacktivist threat was rated the number two risk by our respondents.
- Public perception of the state of cyber insecurity was rated as the third worst perception in the minds of security practitioners.
- Respondents reported continued improvements in information sharing by firms in their industry.

All risk indicators except that for information sharing were up when compared to the previous month.

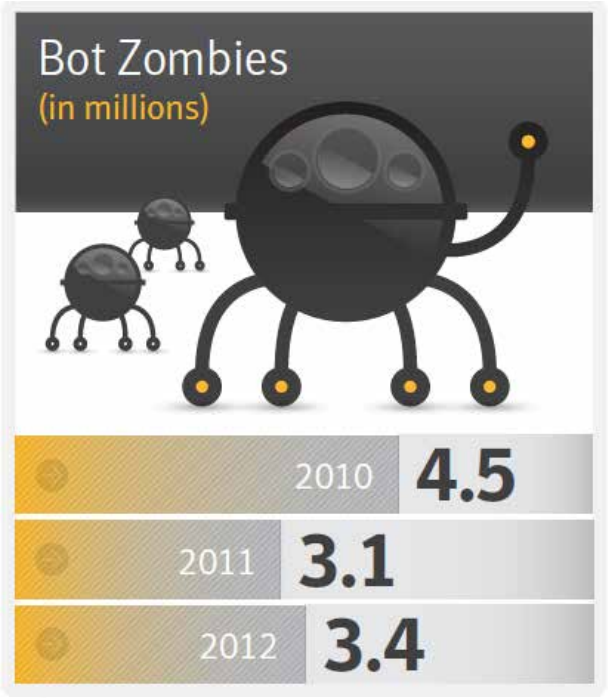
ICS Value, January 2013 = 1599.2 (Base = 1000, March 2011)

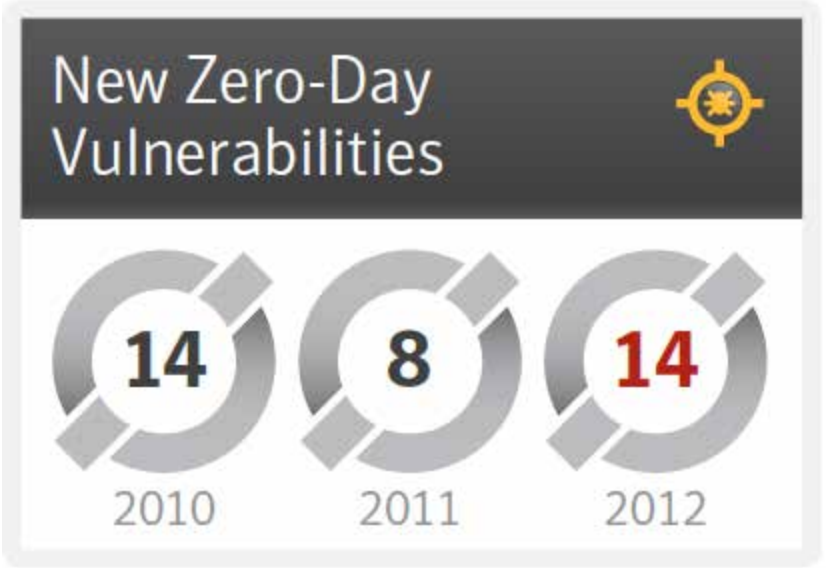
2012 in Numbers

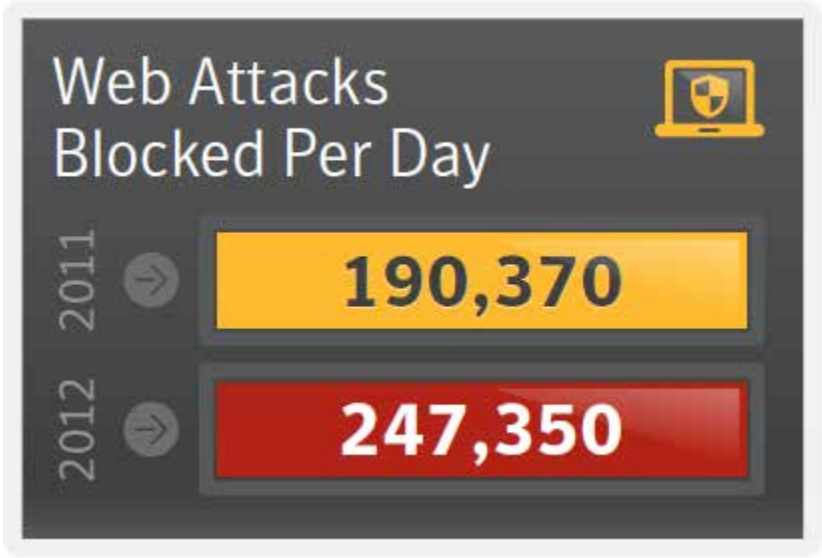


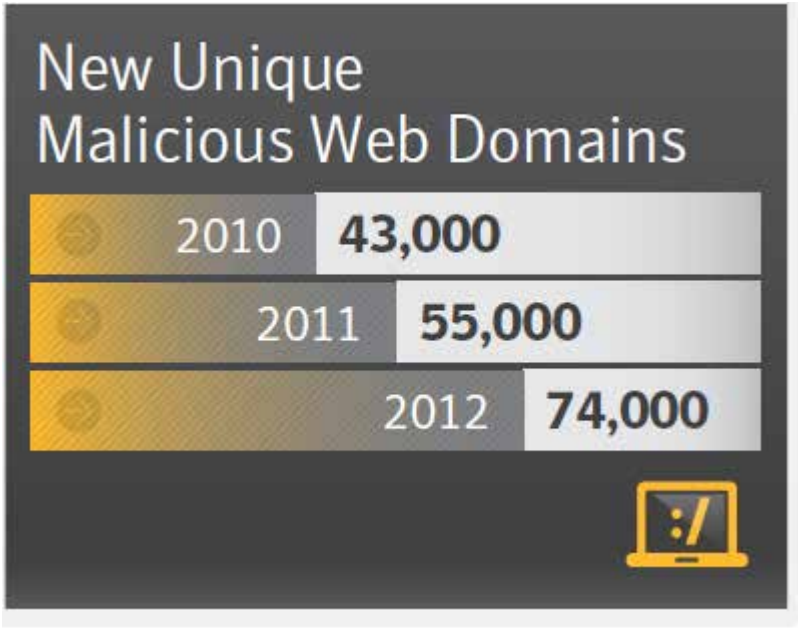


2012 in Numbers









2012 in Numbers

Watering Hole Attacks

1. Attacker profiles victims and the kind of websites they go to.

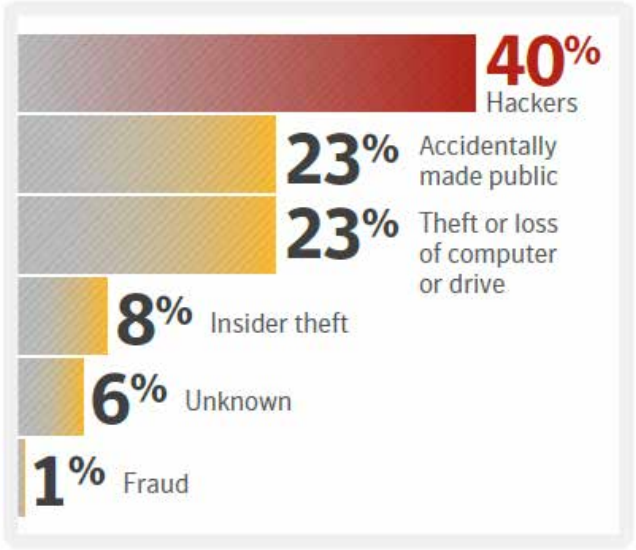
2. Attacker then tests these websites for vulnerabilities.

3. When the attacker finds a website that he can compromise, he injects JavaScript or HTML, redirecting the victim to a separate site that hosts the exploit code for the chosen vulnerability.

4. The compromised website is now "waiting" to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.

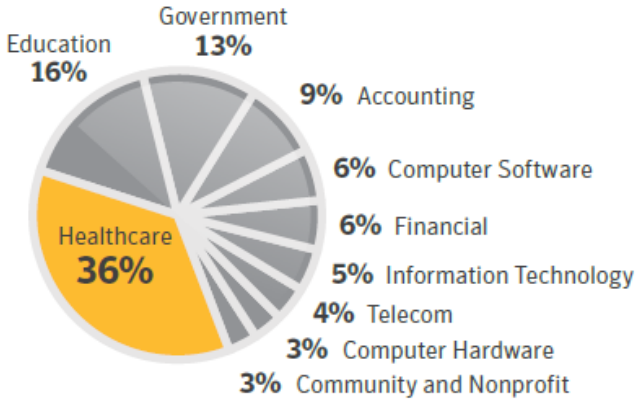
Top Causes of Data Breaches in 2012

Source: Symantec



Data Breaches by Sector in 2012

Source: Symantec

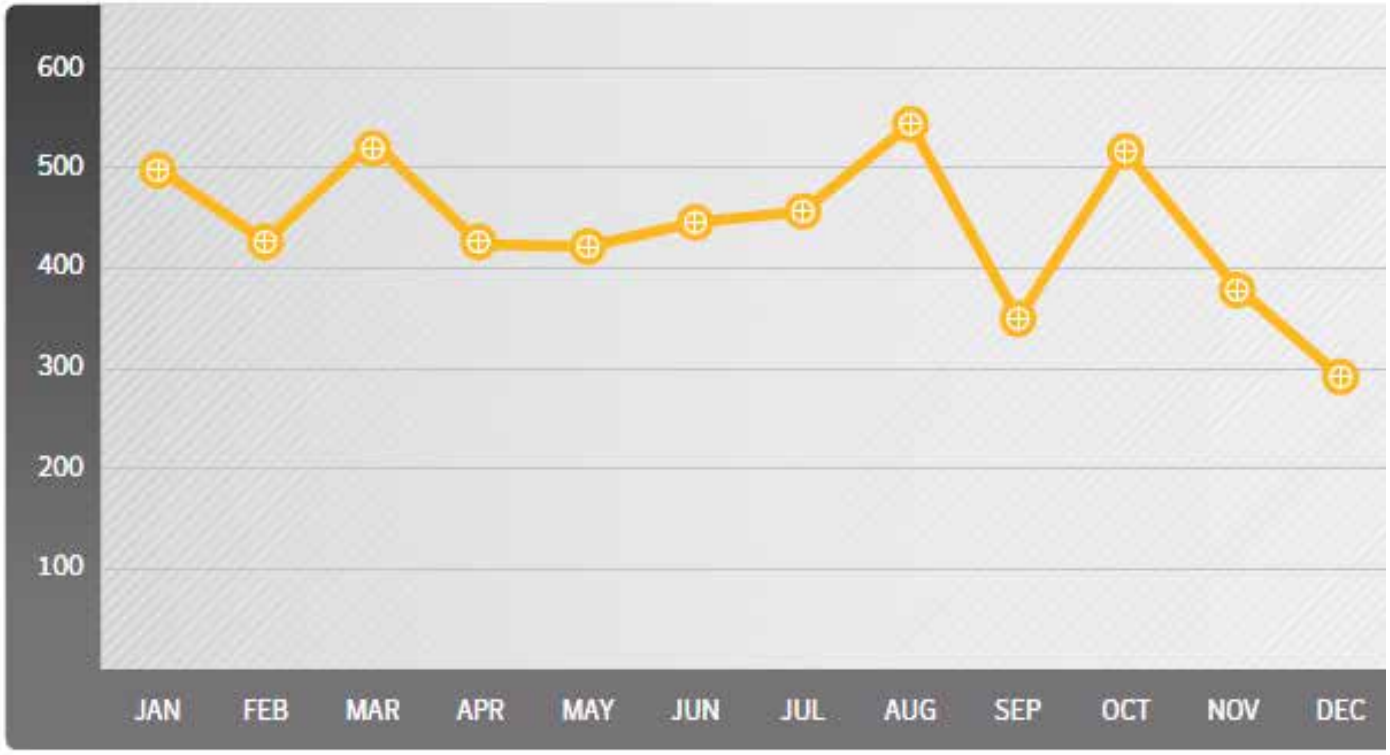


At 36 percent, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industry.

2012 in Numbers

Total Vulnerabilities

Source: Symantec



- *There were 5,291 vulnerabilities reported in 2012, compared with 4,989 in 2011.*
- *Reported vulnerabilities per month in 2012 fluctuated roughly between 300 and 500 per month.*
- *In 2012, there were 85 public SCADA (Supervisory Control and Data Acquisition) vulnerabilities, a massive decrease over the 129 vulnerabilities in 2011.*
- *There were 415 mobile vulnerabilities identified in 2012, compared with 315 in 2011.*

2012 in Numbers

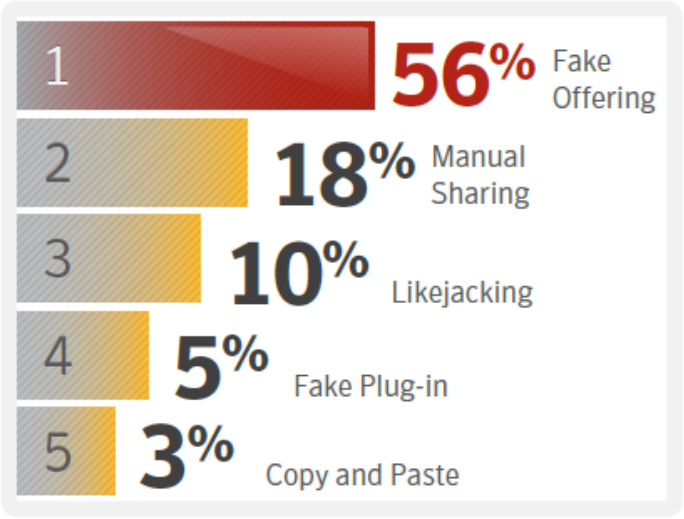
Mobile Threats in 2012

Source: Symantec

Typical social media scam.

Top 5 Social Media Attacks in 2012

Source: Symantec



- **Fake Offering.** These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.
- **Manual Sharing Scams.** These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.
- **Likejacking.** Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.
- **Fake Plug-in Scams.** Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.
- **Copy and Paste Scams.** Users are invited to paste malicious JavaScript code directly into their browser's address bar in the hope of receiving a gift coupon in return.

Mobile Phones: A New Source of Data Breaches

- Mobile devices contain work and personal information
- Unlike a desktop computer they are easily stolen
- …. and often lost

Only 50% of finders attempted to return the phones.

96% of all phones had personal and business applications accessed

Cybersecurity Risk – Mobile Devices

Over half of consumers using smart mobile devices employ location-based applications despite concerns about safety and 3rd party use of their personal information. Almost half state that they don't read agreements when downloading apps. Add that to the fact that few organizations keep track of what type of devices access organizational resources. More than 60% of organizations surveyed allow their personnel to bring their own smart devices to work and access organizational IT infrastructure. So organizations are allowing access to their IT infrastructure by mobile devices used by employees who download applications without understanding their consequences.

Cybersecurity Risk – Mobile Devices

BYOD – Bring Your Own Device to Work
More and more companies are allowing their employees to use their personal smartphones, tablets and computers for work, logging the devices on their business networks and databases. But without significant upfront planning and using the appropriate tools, **this can introduce significant risks to your business and even to the employees.** This risk is to your corporate data and employee personal information.

The biggest risk is that each of these devices has its own operating system. Hackers can go after different OSs differently since **all OSs have different vulnerabilities**. In a survey by Search Mobile Computing, 70% of businesses indicated that loss or theft of mobile devices was the top security concern. Yet, **only half** of companies participating in the survey had a policy requiring power-on passwords, and **just 41%** enforced the policy.

Hackers can find it easier to introduce malware onto employees devices because it is hard to enforce company security software on something not the company's property. Patching their software with the latest security patches is also questionable since the company IT folks can't look into personal devices. ***It's hard to enforce social engineering policy and to limit what web sites are accessed on personal devices.***

Cybersecurity Risk – Mobile Devices

Interesting thought – some mobile devices are just now coming into widespread use – wireless medical devices both worn and implanted. These CAN be hacked.

Also, we are seeing attacks on mobile devices that enable conversations to be listened to and recorded even **if the mobile device is not "on".**

Laptops and PCs can be hacked and the webcam and microphone **turned on remotely**.

Over half of consumers using smart mobile devices employ location-based applications despite concerns about safety and 3rd party use of their personal information. Almost half state that **they don't read agreements** when downloading apps. Note that smart phone photos are imprinted with the current GPS coordinates **unless that feature is turned off.**

Cybersecurity Risk – Mobile Devices

Navigation-and-emergency-services company OnStar is notifying its six million account holders that it will keep a complete accounting of the speed and location of OnStar-equipped vehicles, even for drivers who discontinue monthly service.

OnStar does not currently sell anonymized customer data, but it reserves that right. Both the new and old privacy policies allow OnStar to **chronicle a vehicle's every movement and its speed.** "What's changed [is that if] you want to cancel your OnStar service, we are going to maintain a two-way connection to your vehicle unless the customer says otherwise. Canceling customers must opt out of the continued surveillance monitoring program, according to the privacy policy.

An example of how the data might be used would be for a Department of Transportation "to get a feel for traffic usage on a specific section of freeway." The policy also allows the data to be used for marketing purposes by OnStar and vehicle manufacturers.

Collecting location and speed data via GPS might also create a treasure trove of data that could be used in criminal and civil cases. One could also imagine police acquiring the data to issue speeding tickets en masse.

Cybersecurity Risk – Mobile Devices

Google's Android is the most heavily targeted mobile operating system by malware since it is an open platform where malicious apps can make easy way to users' devices.

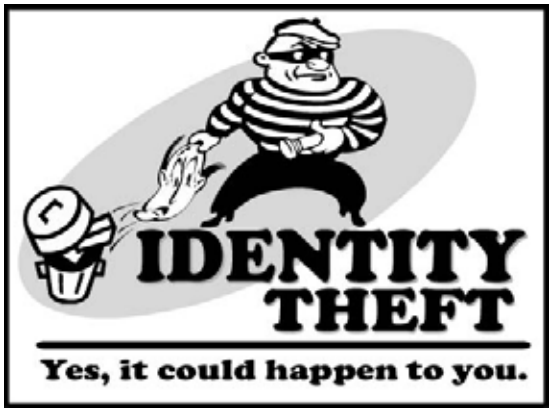
In Q2 2012 5,033 pieces of malicious Android software were received by one security company, which represented a massive **64% increase** of Android malware over **Q1 2012**. This figure placed Android at the top of the list of the highest targeted mobile platforms at present. Most of these are coming from third-party Android markets. Out of the 5033, this company identified 19 new families and 21 new variants of existing families.

To protect your phone, use common sense. If you're downloading applications, look at the info you have available — user ratings, the developer, the number of downloads. If there's an app with few user comments and few total downloads, and it's released by a developer you never heard of, steer clear. If you see a free game or entertainment app that collects phone call, location and contact data, you should skip it. For Android, the danger is downloading apps outside of Google's App Market (or other reputable app stores such as Amazon's). If you're off somewhere getting apps from sources you don't know or trust, there could be consequences. For iPhone users, the line really is whether you jailbreak or not. Jailbreaking can be pretty easy, and getting pirated or bootlegged apps can seem like a great way to save money, but in doing so, you're basically handing out the smart phone equivalent of a front door key to someone . ***Just realize that are bad things out there.***

Cybersecurity Risk – Identity Theft

More than 93 million identities were exposed in 2012 by data breaches, but most of the breaches are linked to ***old-fashioned theft (like a stolen laptop) and/or sloppy security*** rather than to hacking. Top ten sectors for data breaches in 2011-

36% - Healthcare;
13% - Government;
16% - Education;
6% - Financial
9% - Accounting;
6% - Computer Software;
5% - IT;
4% - Telecom
3% - Computer Hardware;
3% - Community and Nonprofit



A scam that hit much of the country in June has now reached utility customers in Alabama, natural gas company Alagasco and the Better Business Bureau of Central Alabamanoted. Scammers have been going door-to-door and using text messages, social media and handbills to solicit personal data such as social security numbers. The scammers claim that a grant program authorized by President Barack Obama will pay their utility bills, if they provide the personal data.

Cybersecurity Risk – Identity Theft

Identity thieves are targeting children – it's the crime of opportunity and is often committed by someone in the family. Children are targeted 35 times more than adults, with 15% under the age of 5. This crime tends to go undetected until victims turn 18 and try to get a student or car loan and discover they already have a credit file. All that is required is an SSN, birthday, addresses and parent's names. Since the Social Security verification service can only be used for W-2 reporting purposes, banks verify SSNs, names and birthdates with credit bureaus. So keep your kid's SSNs, birthdates, etc. information close hold, ***DON'T*** put it on Facebook or MySpace.

Approximately ***15 million United States residents*** have their identities used fraudulently each year with financial losses totaling upwards of $50 billion. On a case-by-case basis, that means approximately 7% of all adults have their identities misused with each instance resulting in approximately $3,500 in losses. These alarming statistics demonstrate identity theft may be the most frequent, costly and pervasive crime in the United States.

IRS Overwhelmed by Tax Related Identity Theft

Phoebe Putney Memorial Hospital in Albany is warning patients that their personal information might have been accessed by a former nurse accused of identity theft. Melody Milton was charged in April with stealing the identities of people and filing more than $1 million worth of false tax returns.

The IRS increasingly struggles to control taxpayer identity theft. Since 2008, the IRS has identified 470,000 incidents of identity theft affecting more than 390,000 taxpayers. “Victims of tax-related identity theft are the casualties of a system ill-equipped to deal with the growing proficiency and sophistication of today’s tax scam artists” said Sen. Bill Nelson, who chairs the newly formed Subcommittee on Fiscal Responsibility and Economic Growth.

Identity theft harms innocent taxpayers through (1) employment and (2) refund fraud, according to the GAO. In refund fraud, an identity thief uses a taxpayer’s name and Social Security number to file for a tax refund, which the IRS discovers after the legitimate taxpayer files. In the meantime, the victim is out the money due him/her. You must painstakingly prove your identity to the IRS, normally time after time over a several-month period, often 10 -15 months. ***For many people this has happened more than once.***

IRS Overwhelmed by Tax Related Identity Theft

How do you know if your tax records have been affected?

Usually, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season. You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

Be alert to possible identity theft if you receive an IRS notice or letter that states that:

- More than one tax return for you was filed,
- You have a balance due, refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages from an employer unknown to you.

IRS Overwhelmed by Tax Related Identity Theft

What to do if your tax records were affected by identity theft?

If you receive a notice from IRS, respond immediately. If you believe someone may have used your SSN fraudulently, please notify IRS immediately by responding to the name and number printed on the notice or letter. You will need to fill out the IRS Identity Theft Affidavit, Form 14039. For victims of identity theft who have previously been in contact with the IRS and have not achieved a resolution, please contact the IRS Identity Protection Specialized Unit, toll-free, at 1-800-908-4490.

How can you protect your tax records?

If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity or credit report, etc., **contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.**

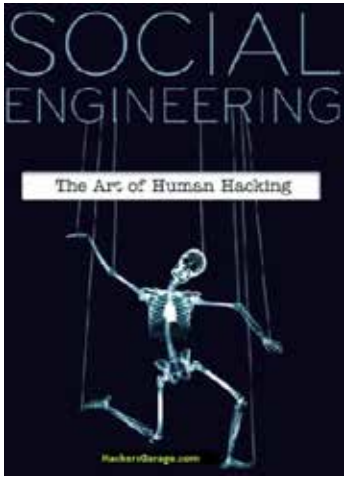
Cybersecurity Risk - Extortion

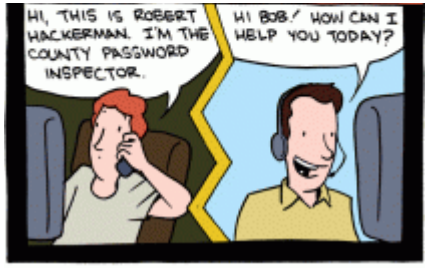
Scammers (extortionists) are requiring a payoff or discount from retail stores or restaurants or they will post a terrible rating on online review sites. Legal experts say that not to pay and not to file a lawsuit is wise. If a business is seen as litigious, it can be as bad for your reputation. The best course is to use the same social media to explain your side of the story and work for more positive reviews. Victims of cyber extortion can't blame the online sites. Review sites are not legally responsible for what their users do.

Cybersecurity Risk – Social Engineering

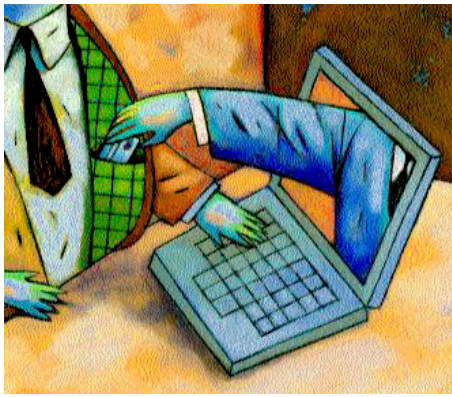
Social engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Fraudsters are perfecting their abilities to target and manipulate people. Well-crafted social engineering schemes take advantage of common user behavior. Don't click on unknown links or provide personally identifiable information to someone you don't positively know. A call from "the IT department" asking for your password to check some obscure area of the computer system works wonderfully well.





Cybersecurity Risk – Fraud/Phishing



Phishing and Smishing Schemes
In **Phishing schemes**, a fraudster poses as a legitimate entity and uses e-mail and scam websites to obtain victims' personal information, such as account numbers, user names, passwords, etc. **Smishing** is the act of sending fraudulent text messages to bait a victim into revealing personal information.

Be leery of e-mails or text messages that indicate a problem or question regarding your financial accounts. In this scam, fraudsters direct victims to follow a link or call a number to update an account or correct a purported problem. The link directs the victim to a fraudulent website or message that appears legitimate. Instead, the site allows the fraudster to steal any personal information the victim provides.

Phishing schemes related to deliveries are also rampant. Legitimate delivery service providers neither e-mail shippers regarding scheduled deliveries nor state when a package is intercepted or being temporarily held. Consequently, e-mails informing of such delivery issues are phishing scams that can lead to personal information breaches and financial losses.

Cybersecurity Risk – Fraud/Phishing

Phishing is difficult to detect because it contains official-looking logos and other identifying information from legitimate organizations. A phishing e-mail normally starts with a generic greeting, such as “Dear Customer” or “To our valued client.” Phishers send out millions of messages to randomly generated e-mail addresses hoping that people who can relate to the message would reply to them. Banks personalize their greetings and indicate your full name when sending official correspondence.

Most phishing e-mails include threats requiring immediate action. They contain phrases such as “Verify your account, “Update your account,” and “Failure to do so will result in account suspension.” Mainly all phishing scams will request your personal information. Most legitimate banks will not demand this information online or through e-mail.
If you receive an e-mail or pop-up message from your bank or credit card company or from businesses that you regularly transact with such as eBay or Amazon and you suspect it is a phishing scam, do not reply to it. ***Just ignore and delete the message***.

The primary way to avoid phishing scams is to educate yourself.

Cybersecurity Risk – Fraud/Phishing

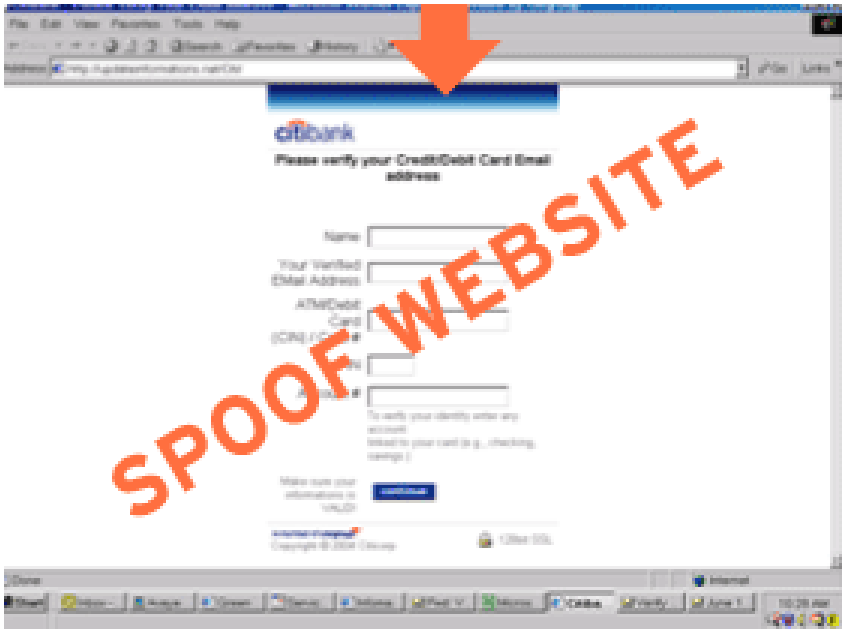
Phishing and Smishing Schemes

Current **smishing** schemes involve fraudsters calling victims' cell phones offering to lower the interest rates for credit cards the victims do not even possess. If a victim asserts that they do not own the credit card, the caller hangs up. These fraudsters call from TRAC cell phones that do not have voicemail, or the phone provides a constant busy signal when called, rendering these calls virtually untraceable.

Another scam involves fraudsters directing victims, via e-mail, to a spoofed website. A spoofed website is a fake site that misleads the victim into providing personal information, which is routed to the scammer's computer.

The best way to avoid phishing is by knowing what to look for and to NOT give out any personal information to anyone unless you absolutely know who you are giving your information to.

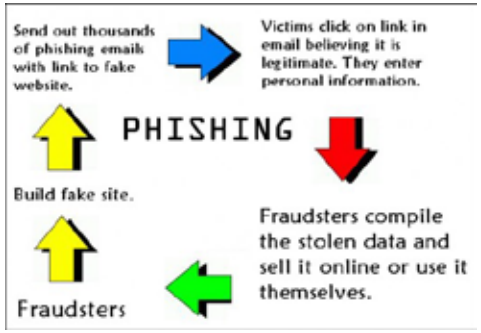
Spoofed Website



A Spoofed Website is site which is made similar to a real website - usually joined with phishing scams. There are ways to determine a spoofed website.

1. The best way to find out a Spoofed Website is checking the websites certificate. Update your web browser regularly, older versions of browsers can be easily hacked. New browsers are very secure which can avoid scams, viruses, Spoofed Websites, etc
2. Be aware of cybersquatting. Cyber criminals open a website ***similar*** to a real website for earning cash through advertisements. These kind of websites are illegal and normally contain viruses.
3. Bookmark websites you go to often and avoid opening them from e-mails or possible mistyping.
4. Always use an antivirus program to alert you if a site may contain malicious programs or virus.
5. Check if a website is secure by checking if the URL begins with an “https” and if a closed padlock icon is displayed on the browser’s status bar. To confirm authenticity of the site, double-click on the lock icon and review the security certificate information it will display.

Cybersecurity Risk – Fraud/Phishing



A massive phishing and fraud scheme that targeted Bank of America, Chase Bank and payroll processor ADP defrauded them of $1.5 million. The phishing attacks directed users to spoofed or fake web pages designed to mimic legitimate sites. Once on the spoofed sites, users were conned into entering confidential personal and financial information. These stolen usernames and passwords were used to hack and compromise accounts as well as initiate unauthorized transactions and withdrawals. The phishers also created fake drivers licenses, access online accounts (viewed online checks to find out how to forge signatures) and access payroll accounts at ADP. They added fake employee accounts to company payrolls and had paychecks issued to the fake employees. ***Social engineering schemes are getting much more sophisticated.***

Subject: ANZ Account Suspension
Date: 7:48 AM
To: brettmalcom@bigpond.com

From: "ANZ Banking" Reply-To: "ANZ Banking"

Scam Message

ACCOUNT SUSPENSIO

In an effort to protect your ANZ Banking account security, we have suspended your account until such time that it can be safely restored by you.

We have taken this action because your ANZ online account may have been compromised, Someti this h ens when members respond to tropans,worms and other effected virus files. Althou ca sclose our investigative procedures that led to this conclusion, Please th to ti te th of unt

To com t a rat process for ccoun or acc ,p se c h https: w z /i ai

Thank You.

Accounts Management As outlined in our User Agreement, Australia and New Zealand Banking Group Limited (ANZ) will periodically send you information about site changes and enhancements.

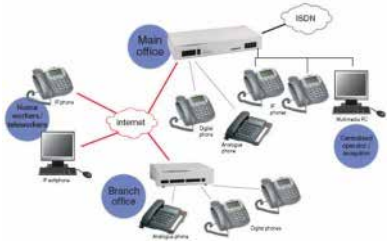
Visit our Privacy Policy and User Agreement if you have any questions.
ANZ Web Site Security and Privacy Statement

Social Engineering – It Works!

Fake Tech-Support Calls

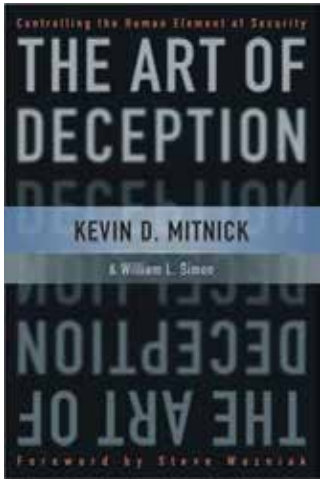
You might get an unsolicited phone call from a tech-support representative claiming to be from Microsoft or another big-name IT corporation. But the caller won't be who he claims to be. After warning you that "**suspicious activity**" has been detected on your computer, he'll offer to help — once you give him the personal information he requires to get his job done.

That job isn't fixing your computer. In fact, he's really just after your personal information. If you receive a call like this, hang up, call the company the bogus technician claimed to be from, and report the incident to a legitimate representative. If there really is a problem, they'll be able to tell you; if not, you just thwarted a data thief.



Classic Examples of Social Engineering Attacks

Baiting - Much like a bait car is used to attract automobile thieves, a bait disk or bait drive is left in the open for a target to find. Succumbing to curiosity, the target attempts to read the disk and thereby infects his computer with malware.
Defense Against Baiting - Don't access that disk, you don't know where it's been.



Phishing – False emails, chats or websites designed to impersonate real systems with the goal of capturing sensitive data. The classic examples are a mocked-up login page that steals your username and password, or an email requesting you reply to confirm your personal information.
Defense Against Phishing – Your password doesn't get entered anywhere but your login page, and that page better have the right URL.

Pretexting - The human equivalent of phishing, where someone impersonates an authority figure who is entitled to access your login information. The fake IT staffer asking for your password to do system maintenance, or the false investigator performing a company audit are two typical pretexting examples.
Defense Against Pretexting – ***Nobody needs your password, ever.***

Classic Examples of Social Engineering Attacks

Quid Pro Quo – A system that requests your password or personal information in exchange for some compensation. Previously, these took the form of contests — share your password to win a free t-shirt — but increasingly resemble application install or download forms where the user is prompted to share login credentials to access an online game or service.
Defense Against Quid Pro Quo – ***Nobody needs your password, ever.***

Tailgating – Following someone into a restricted area or system. In physical attacks, this could simply mean passing through a security door at the same time as a legitimate entrant, as in "can you hold the door?" or similar exploitations of courtesy. In the context of the cloud, this typically means using a device that is already logged into an online app, such as when an attacker asks to borrow a phone or laptop to "check email" but surreptitiously performs malicious acts instead.
Defense Against Tailgating – ***Nobody other than you uses your computer (or tablet, or phone) while you're logged in, ever.***

Common Scams Used in Social Engineering

1. **Quizzes, polls and contests** – The promise of something for nothing is a classic scam. One promises that the first 20 responders will receive $1,000 gift cards to a popular electronics store if they "like" the store on Facebook. Clicking on the link in the e-mail will take you to a bogus page that asks for numerous personal details – basically identity theft – and there is no gift card.

To protect yourself ignore these kinds of offers or go directly to a company's Facebook page or website to verify that the offers are legitimate.

2. **Auctions and Deals To Good To Be True** – Shopping at online auctions and classified ad sites can be useful, but ***NOT*** if the seller wants you to wire money in advance.

To protect yourself remember the old sayings "If it's too good to be true, it probably is". Thoroughly check out a seller's ratings and reviews before you bid on any online auction. Some fraud sites actually imitate a BBB seal or offer phony positive reviews to throw you off. Verify BBB approval at BBB.org. Whatever you do, ***NEVER*** pay by wire transfer as this is a surefire indication of a fraudulent sale.

Common Scams Used in Social Engineering

3. **Phony Do-Gooders** – After any disaster, scammers try to take advantage of our good nature and generosity by asking for donations via a website or text message and then keeping the money for themselves.

To protect yourself check if a charity is legitimate at the BBB Wise Giving Alliance or American Institute of Philanthropy websites. Or donate directly through a known charity's web site.

4. **Malware-ridden e-cards and Programs** – Animated cards, games and screen savers never go out of style. Scammers take advantage of user's boredom and trick them into downloading applications laden with spyware and other malware.

To protect yourself, use a strong anti-malware product. That will usually stop malware in its tracks. But your best bet is ***not to open any e-mail attachment*** – even from someone you know – if you aren't certain it is legitimate. Check before you click.

Common Scams Used in Social Engineering

5. **Vacation Homes (Not Really) For Rent** – This up and coming scam is simple – a fraudster sets up a vacation rental site for a real home (complete with photos) and they rent it out for weekend and holiday getaways. The problem is that the scammer doesn't own the house, its not actually for rent, and when you get there, the owner doesn't know anything about it.

To protect yourself use only trusted travel sites and rental agencies when booking. Low-resolution photos of the home and super-low rental prices are giveaways that something is fishy.

6. **Fake E-Mails and Phishing Trips** – A common trick is an e-mail that "confirms" an order, payment or shipment you know nothing about. The e-mail, which may appear to be from a reputable company, advises you to click on a link or attachment to view the status of the order or shipment. When you click you are routed to a fake website that asks you to enter your personal information – identity theft.

To protect yourself avoid opening e-mails from people and companies you don't recognize or trust. Permanently delete those e-mails. Don't click on links or attachments. Type the web address into your address bar so you go directly to the site. If you are not expecting a shipment, delete the e-mail. If you receive an order or payment contact the company directly.

The Nigerian E-Mail Scam

You've seen the e-mail – some terminally ill Nigerian prince or General or the Director of a large corporation contacts you urgently asking you to move a large sum of money, promising you a share. All they need are your credit card number or bank account info.

But who on earth actually believes these e-mails? Doesn't matter. Those of us who wonder are not the target. A recent study found that the scammers aren't interested in being too believable because it would be too expensive if everyone fell for it. So the e-mail is designed to eliminate anyone intelligent, leaving only the most gullible to hit. It works, last year one Nigerian man was jailed after scamming $1.3 million.

ADVERTISEMENT ADVERTISEMENT ADVERTISEMENT ADVERTISEMENT

CENTRAL BANK OF NIGERIA

PRESS STATEMENT ON ADVANCE FEE FRAUD/SCAM

DON'T BE FOOLED! MANY HAVE LOST MONEY!!

IF IT SOUNDS TOO GOOD TO BE TRUE THEN IT IS NOT TRUE!!!

1 The publicity campaigns by the Central Bank of Nigeria (CBN) and the Government of the Federal Republic of Nigeria have proved successful in sensitising the public about the menace of advance fee fraud and the falsehood of claims that easy money could be made in Nigeria. Consequently, the reported incidence of advance fee fraud (A.K.A. '419'), has declined significantly. Nevertheless, there are still some people who have continued to fall victim to the solicitations of advance fee fraudsters. This warning is, therefore, specifically intended for the benefit of those misguided people who, in the quest to make easy money at the expense of Nigeria, are defrauded by international fraudsters.

2 The advance fee fraud is perpetrated by enticing the victim with a bogus 'business' proposal which promises millions of US dollars as a reward. The scam letter usually promises to transfer huge amounts of money, usually in US dollars, purported to be part proceeds of certain contracts, to the addressee's bank account, to be shared in some proportion between the parties. A favourable response to the letter is followed by excuses why the funds cannot be remitted readily and subsequently by demands for proportionate sharing of payments for various 'taxes' and 'fees' supposedly to facilitate the processing and remittance of the alleged funds. The use of 'fake' Government, Central Bank of Nigeria, Nigerian National Petroleum Corporation, etc. documents is a common practice.

3 The fraudsters usually request that the transaction be done under the cover of confidentiality. Sometimes, the 'victims' are invited to Nigeria where they are given red-carpet reception and attended to by the fraudsters, posing as Nigerian Government officials. Quite often the fraudsters invent bogus Government committees purported to have cleared the payments. Also, it is not unusual for them to contrive fake publications in the newspapers evidencing purported approvals to transfer non-existent funds.

4 To consummate the transaction, the 'victim' would be required to pay 'advance fees' for various purposes: e.g. processing fees, unforeseen taxes, licence fees, registration fees, signing/legal fees, fees for National Economic Recovery Fund, VAT, audit fees, insurance coverage fees, etc. The collection of these 'advance fees' is actually the real objective of the scam!

5 A recent variant of the scam directed primarily at charitable organisations and religious bodies overseas involves bogus inheritance under a will. Again the sole aim is to collect the 'advance fees' already described above. A new strategy that has also been used to defraud the 'victims' is an offer to use chemicals to transform ordinary paper into United States dollar bills, which would be subsequently shared by the parties.

6 You are again warned in your own interest not to become yet another dupe to these fraudulent solicitations or schemes. Genuine and prospective investors in Nigeria are advised to consult their home Chambers' of Commerce and Industry, or Nigeria's Chambers' of Commerce and Industry, Manufacturers' Associations of Nigeria, Federal Ministries of Commerce and Industry, Nigerian Missions in their countries of origin, their embassies or High Commissions in Nigeria for proper briefing and advice.

7 The Central Bank and indeed, the Federal Government of Nigeria cannot and should not be held responsible for bogus and shady deals transacted with criminal intentions. As a responsible corporate body, the Central Bank of Nigeria is once again warning all recipients of fraudulent letters on bogus deals, that there are no contract payments trapped in the bank's vaults. They are once again put on notice that all documents appertaining to the payment, claims, or transfers purportedly issued by the bank, its senior executives or the Government of the Federal Republic of Nigeria for the various purposes described above are all forgeries, bogus and fraudulent.

8 Please join the Central Bank and the Federal Government of Nigeria to fight the criminal syndicates who play on the gullibility and greed of their victims by reporting any solicitation to your local law enforcement agencies or the local International Police Organisation (Interpol).

9 You have been warned several times before! You have been warned again!!

CENTRAL BANK OF NIGERIA

Samuel Ladoke Akintola Way, P.M.B. 0187, Garki, Abuja, NIGERIA

A Kauai woman received several e-mails as part of a Nigerian scam attempting to obtain large sums of money from her. The e-mails contained a photo of a Hawaii County police officer, a Police Department logo and other information that had been cut-and-pasted from the Hawaii Police Department's website in an apparent attempt to mimic official letterhead and impersonate a police officer.

Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money

A new Citadel malware platform used to deliver ransomware named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States federal law. The message further declares the user's IP address has been identified by the Federal Bureau of Investigation as visiting websites that feature child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the U.S. Department of Justice using a Prepaid money card service. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar, do not follow payment instructions. Infected computers may not operate normally. You can file a complaint at **www.IC3.gov** . Seek out a local computer expert to assist with removing the malware.

E-Mails Containing Malware Sent to Businesses Concerning Their Online Job Postings

Recent FBI analysis reveals that cyber criminals engaging in ACH/wire transfer fraud have targeted businesses by responding via e-mail to employment opportunities posted online. Recently, more than $150,000 was stolen from a U.S. business via unauthorized wire transfer as a ***result of an e-mail the business received that contained malware***. The malware was embedded in an e-mail response to a job posting the business placed on an employment website and allowed the attacker to obtain the online banking credentials of the person who was authorized to conduct financial transactions within the company. The malicious actor changed the account settings to allow the sending of wire transfers, one to the Ukraine and two to domestic accounts. The malware was identified as a Bredolab variant, svrwsc.exe. This malware was connected to the ZeuS/Zbot Trojan, which is commonly used by cyber criminals to defraud U.S. businesses.

The FBI recommends that potential employers ***remain vigilant in opening the e-mails of prospective employees***. Running a virus scan prior to opening any e-mail attachments may provide an added layer of security against this type of attack. The FBI also recommends that businesses ***use separate computer systems to conduct financial transactions.***

Protect Personal Information When Seeking Employment

Phishbucket.org – an online clearinghouse of job scam information – states that ***the number of reported job scams tripled between 2008 and 2010***. Protect yourself by:

1. Never put the following on your resume if you intend to post it – SSN, driver's license number and date of birth. Also don't put it on job applications. Consider writing "prefer to provide this information during the interview".

2. Not all career websites are created equal. Be sure that you review the privacy policy and user terms and agreements before you post your resume. If in doubt check with The World Privacy Forum's Consumer's Guide to Online Job Sites.

3. You might be looking at a fake job ad if it offers considerable pay with few to no duties, promises payment of wages in cash, contains no physical address or contact person and/or requires you to open a new bank account or accept company checks to "test" a wire transfer service.

Protect Personal Information When Seeking Employment

4. Carry good data security practices with you offline – other vulnerable situations include phone interviews, job fairs and e-mail and phone conversations with recruiters. As long as someone thinks an offer is genuine, they are more likely to provide sensitive information. Know who you are talking to. **Virtually all legitimate businesses or recruiters will NOT ask for your SSN or other personal information until after you have begun a formal interview process.** A legitimate company should not ask for you to divulge personal identifiers via e-mail as e-mail is not secure.

5. Think before you post to a social media site. The more you reveal online, the greater the chance of having the information accessed by identity thieves. ***Remember this*** – if you wouldn't give this information to a stranger on the street, you probably don't want to put it online for the world to see.

6. Secure your delivery channels. Make sure your computer or other device you use is equipped with antivirus and antimalware programs. And ***don't use a Public WI-FI to transmit data.***

Cybersecurity Risk – Data Breach

What we've learned from other data breaches where hackers got into company databases is that you re-use your passwords a lot. Here were the most common passwords:

1. 123456 2. 12345 3. 123456789 4. Password 5. iloveyou 6. princess
7. rockyou 8. 1234567 9. 12345678 10. abc123 11. Nicole 12. Daniel
13. babygirl 14. monkey 15. Jessica 16. Lovely 17. michael 18. Ashley
19. 654321 20. Qwerty

But even if your password isn't on the list, the online privacy and identity theft problem here is **DATA MINING**. Hackers are good at cross-referencing data. They can take 50 million names and emails from Epsilon, compare that with 32 million emails and passwords from Rockyou (and other breaches and fake phishing sites), and get hundreds of thousands of online accounts with which they can commit fraud. ***It's basically child's play.***

This is why everyone needs to take care not to get too angry at Epsilon, ***but get in control of your online privacy.***

Cybersecurity Risk – Data Breach

Thousands of passwords and credit card details have been exposed online after social engineers breached popular hosting billing platform WHMCS. ***Attackers obtained the data after masquerading as the platform's lead developer, Matt Pugh. Attackers managed to con the company's hosting provider to release administrator credentials.***

Pugh's details were then used to access WHMCS' database and steal hashed customer credit card numbers and passwords, usernames and support tickets. That data along with the WHMCS control panel and web site information was dumped online in a 1.7 gigabyte cache. Links to the cache and other, smaller files were tweeted under the WHMCS Twitter account, which the attackers also hijacked.

Almost a day's worth of data was erased from the compromised servers, including "any tickets or replies submitted within the previous 17 hours."

Cybersecurity Risk – How Can You Lose Your Data?

Credit/Debit Systems - Four Steps for Protecting Customer Data

The Payment Card Industry Security Standards Council released a set of security standards to be followed by any business accepting credit and debit card payments. If a small business owner is not able to prove that they are PCI compliant by these standards and there is a data breach, ***then the small business can be fined for each instance of the breach.*** The fines can be extremely excessive and for some businesses they could put them out of business.

1. Visit PCIStandards.org and determine your merchant level.
2. Identify your validation type.
3. Pass a vulnerability scan. You must have proof of this scan in order to be compliant.
4. Obtain a certificate of Attestation. Once all else is done, you need to obtain a certificate from the PCI Security Standards Council. This must be done yearly.

And remember, this is an ongoing process. As your credit processing increases or you add new methods of payment your standards will change.

Cybersecurity Risk – How Can You Lose Your Data?

Scareware or Fake Security Software

Security intelligence gathered by Microsoft Corp shows a significant increase in rogue security software or ‘scareware’ that lures people into paying for protection that, unknown to them, is actually malware often designed to steal personal information. Individuals are warned not to follow advertisements for unknown software that appears to provide protection and should avoid opening attachments or clicking on links to documents in e-mail or instant messages that are received unexpectedly or from an unknown source.

Cybersecurity Risk – How Can You Lose Your Data?

Pin Skimming

At Chase Bank in Manhattan, East Village.
A customer inserted his ATM card into one of two side-by-side automatic teller machines. When the machine told him it could not read his card, it took him a bit of jiggling to get his card back. He tried it a couple more times and got the same results. Before trying the other machine, he inspected the slot of the current ATM he was using and realized that it had a false plastic cover attached to the slot.

The amazing thing about the cover was that the translucent green plastic matched the card reader slot perfectly, meaning that it was made specifically for Chase ATMs. After snapping a few photos with his iPhone, he alerted the branch manager and explained what happened. The customer went back to the ATM to inspect, which is where he found an extra mirror attached to the vandalized machine that the other ATMs didn't have. Drilled into the mirror was a tiny pinhole with a camera inside, directed at the PIN pad. The customer asked Chase why they hadn't inspected the ATM. Chase honestly replied that they hadn't thought of it because they had never encountered that sort of thing before.

Cybersecurity Risk – How Can You Lose Your Data?

Pay-at-the-pump terminals and ATMs also rank high in the skimming chain because they are unattended. They are usually a fraudsters' easiest target. Pay-at-the-pump has proven vulnerable because of easy accessibility. **Default codes** used to open gas pump enclosures have been exploited by criminals posing as technicians, for instance. Once inside, the criminal can install a skimming device and connect it directly to the terminal's key pad and card reader. It's undetectable from the outside, giving the device ample opportunity to collect card data in real-time, as the card is swiped and PIN entered.

Chase Bank branches in and around Las Vegas have found card skimmers *on their doors*, enabling thieves to capture bank card info without tampering with the ATM at all. At the cash machines, all the thieves need are pinhole cameras to record the PINs.

Cybersecurity Risk – How Can You Lose Your Data?

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION: PRIVACY, SECURITY, TRANSACTIONS

How Much Protection Does Your Data Need?

HIPAA compliance requires training of almost all individuals who work for a healthcare organization – even those who may only be incidentally exposed to such information. Examples of people who should be trained in the HIPAA regulations (in the basics of patient privacy and confidentiality including concepts such as "Protected Health Information" (PHI) and the "Minimum Necessary" principle) include:

- physicians, chiropractors, nurses, technicians, administrators, clerks, order processing staff , staff employees such as custodians, transportation, security , volunteers, independent contractors, consultants and vendors

And the rules also require that these training programs are fully documented.

Top HIPPA Security Rule compliance issues are: inadequate user activity monitoring; inadequate contingency planning; insufficient authentication and integrity of data; media reuse and destruction; not conducting regular risk assessments and inadequate monitoring of granting or modifying user access. (Dept of Health and Human Services Office for Civil Rights audit effort, May 2012

Data Protection Priorities –
ISO 27000 Compliant
Sarbanes Oxley Compliant –
HIPAA Compliant
Privacy Act Compliant

Risks in Use of the Cloud

One of main reasons organizations adopt cloud applications is to free their employees from the constraints of a physical network. With cloud apps, you don't have to log into a work-issue PC attached to a corporate LAN in a company office to get your information or do your job. Any web-connected computer will do, so efficiencies and opportunities abound.

This same freedom also applies to hackers of all varieties, but in particular social engineering attackers. Compromised passwords can now be employed from any web-connected PC; the attacker need not enter your building to steal or destroy data. Your employees can be conned in favorable settings — a coffee shop or airport lounge — without the oversight or support of company security staff. Above all, it is much easier for an attacker to pose as a legitimate authority when their target is already accustomed to dealing with remote teammates via phone, email or chat. If you've never met your IT staff, it's far simpler for a hacker to pretend to be from that IT staff.

Risks in Use of the Cloud

User error is the leading cause of data loss in the cloud. This is due in equal part to the cloud's extraordinary hardware redundancies and to the radical expansion of access afforded by online applications. ***Social engineering attackers hit your system at its weakest point — your people.***

Are your business processes suitable for moving to the Cloud? What happens if access goes down for a prolonged period? Do you have special regulatory and security requirements for specific types of data? Have you developed responses to these requirements for each type of data or do you use one overall requirement? ***When information resided on your computers, data loss was your problem. When your information resides in the cloud, it is still your problem.***

Dangerous Malware

Banking Trojans

The ZeuS Trojan and its rival SpyEye take advantage of security holes in your Internet browser to "piggyback" on your session when you log in to your bank's website. They avoid fraud detection using caution, calculating inconspicuous amounts of money to transfer out of your account based on your balance and transaction history.

While financial institutions continue to increase the layers of security involved in large transactions, such as requiring confirmation through "out-of-band" communications — such as your mobile device — digital crooks have lost no time adapting to the changes, with ***banking Trojans able to change the mobile number tied to your account and intercept that confirmation request.*** Who exactly is a target for these? ***Basically anyone who does not have up-to-date anti-virus or anti-spyware software running on their PC***. Zeus is known to spread through spam emails, infected websites and even downloaded files.

How To Beat The Banking Trojans

Though banking Trojans are getting more sophisticated, you can keep them off your system by running regular scans with up-to-date security software. Don’t click links in emails that claim to be from your bank, and when you go to your bank’s website, use the latest version of your browser and enter the URL manually. If your bank offers extra security tools, use them. In the case of fraud, the bank is less likely to hold you liable if you have used its protection.

Cybersecurity Risk – Cyberweapon

Massive Malware Infects Iranian Computer Systems

Just a month after an online security breach forced Iran's oil network offline, the country has another hacking dilemma. Kaspersky Lab detailed an extensive virus affecting computer systems in the Islamic Republic. Called "The Flame," Kaspersky referred to the virus as ***"the most sophisticated cyber weapon yet unleashed."*** This is "the most sophisticated and powerful cyberweapon to date." It can ***record your keystrokes, record nearby conversations from the computer microphone, can take screen shots, use a wireless Bluetooth connection to receive commands and take the address books out of nearby cell phones, chew up hard drives like a shredder.***

It appears to target individuals rather than a company. Many of the current compromised computers are personal systems being used from home internet connections.

Cybersecurity Risk – Cyberweapon

An Italian researcher has found 14 new zero-day vulnerabilities in SCADA products from 7 different vendors. He already published information about 34 zero-day SCADA flaws in March 2011.

Siemens has found a new and highly sophisticated virus that targets computers used to manage large-scale industrial control systems – manufacturing and utility. It is malicious software designed to infiltrate a system and steal important information about he plant or utility. The problem with this one is that it does not attack the Siemens system but uses an undisclosed **Windows bug** (affecting ALL versions of Windows up to 7) to break into the SCADA system. ***This virus spreads when an infected USB drive is inserted into a computer.*** **This virus could be used to take over a SCADA system and hold it hostage for money or learn how to counterfeit products.**

Yuma Area Water Management System

Cybersecurity Risk – Cyber Incidents

The US critical infrastructure (IT, Commercial facilities, transportation, energy, critical manufacturing, communications, government facilities, chemical manufacturing and water) has experienced a significant uptick in reported cyber incidents. The water sector represents more than half of the reported incidents because they use a remote access platform configured with an unsecure authentication mechanism. In all but 5 of the investigated incidents, implementing recommended security best practices could have deterred the attack, reduced the time necessary to detect the attack or reduced the impact. ***Operational security gaps are people at ALL levels of an organization***, insufficient incident response planning and insufficient control systems risk assessments.

Tips From The Trenches

Here are some tips against Social Engineering Attacks

Warn (And Train) Your Employees (And Your Family)– You'd be surprised how few people even consider the possibility of someone posing as an IT staffer to steal a password, or dropping a bait disk into an elevator. ***Forewarned is forearmed***. An employee/individual that knows what proper security procedures are is much more likely to spot and thwart social engineering attacks.

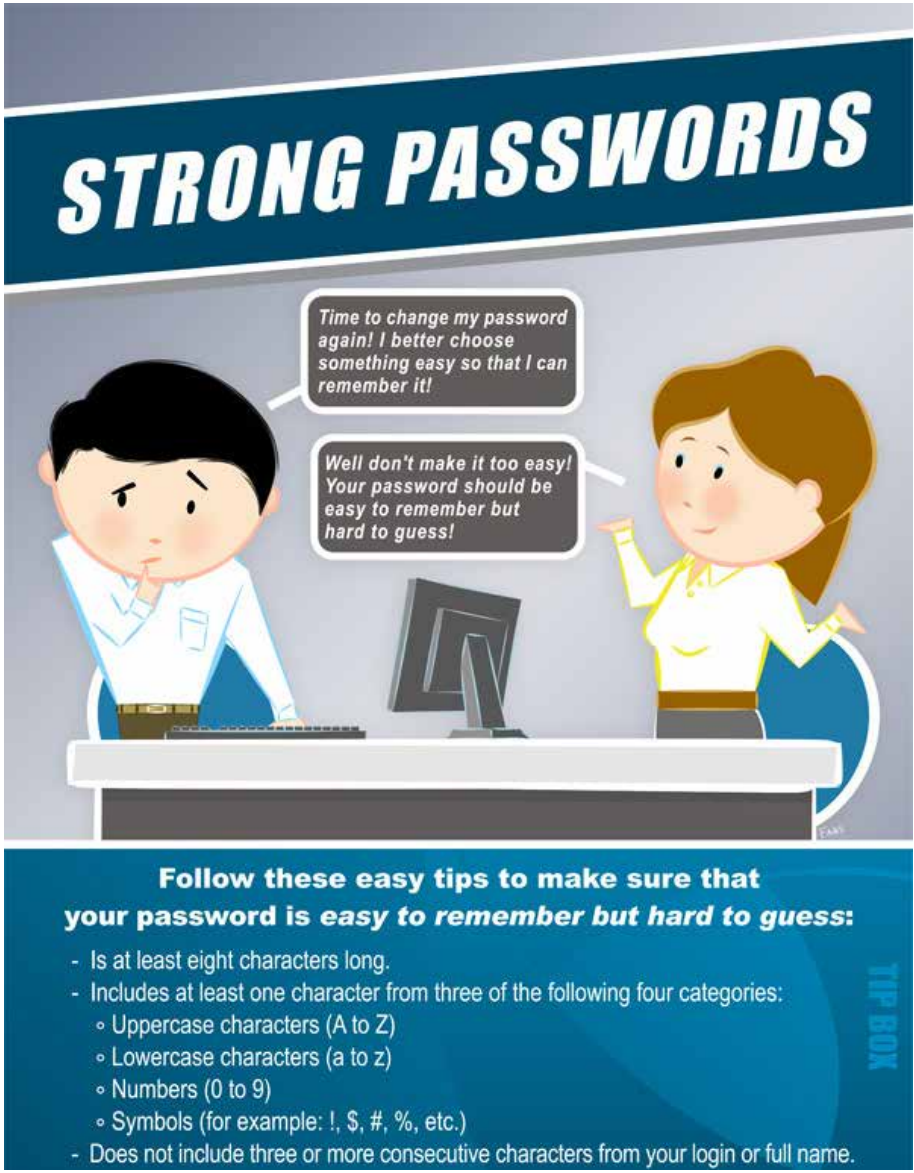
Have A Clear Password Security Policy – A social engineering attacker's greatest asset is uncertainty. If you have a clear "never give out your password" policy, your employees are bound to be more suspicious when someone asks for their credentials. More to the point, virtually all cloud applications give the administrator the ability to reset a password without knowing the existing credentials, so it should be clear to end-users that no IT administrator will ever need their password.

Create A "Culture of Ask" – A culture of double- and triple-checking access requests is always a good idea. Support and security staff should encourage employees to check in whenever access is requested.

Remember, you are the weakest link in your cybersecurity. Unless and until you treat social engineering attacks with the same seriousness as conventional security threats, you put your data, your organization and your family at risk. Train people, be smart about whom you give access to sensitive information and — as always — have a good backup plan.

Tips From The Trenches

- **To secure a network** that allows mobile device connections:
  - ***Require strong password***
  - Have a Password history check
  - Ensure that Passwords expire
  - Inactivity time out
  - Lock out after 7 failed attempts to log in
  - Remote wipe if device is compromised or on lock out
  - Encryption on the mobile device



Tips From The Trenches

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Don’t open e-mails that don’t have subjects.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses and other malware.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail with the link to which you are directed and determine if they match and will lead you to a legitimate site.
- Log directly onto the official website for the business identified in the e-mail, instead of “linking” to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.

Tips From The Trenches

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.
- If you are asked to act quickly, or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.
- Check your credit reports (and all of your families) at least once a year.
- Have someone continually checking the web for your SSN, credit card numbers, account numbers, etc. to show up.
- You should use a dedicated and locked down computer for all online financial transactions.
- Encryption of **ALL** data, regardless of where it is, remains the best prevention idea.
- Always ***KNOW WHO*** you are talking/e-mailing/messaging to and don't provide ANY important information over the phone unless you have initiated the call. The HelpDesk, IT department, IT vendor, phone company, bank, etc. won't call.

Tips From The Trenches

- **Keep Travel Plans Private -** People increasingly broadcast their travel and dinner places on Facebook or Twitter, making thieves aware of empty homes. According to recent surveys, nearly 50% of travelers between the ages of 18 and 34 post their whereabouts as social media updates. Many identity thieves know peak travel or go to dinner times and simply **break into empty homes in search of bank statements, SSN cards, and other important account information**. ***So where is your important information and is it easy to find?*** If it is not secure, you are at higher risk for identity theft. Don't write about where you are or post photos of a trip until you return.
- Just remember – ***Most legitimate businesses or government organizations*** will ***NEVER*** ask you for personal information or business information over e-mail or telephone call (if you did not initiate it).
- Always have backups for any important data/applications.
- The biggest cause of data breaches as lost and stolen computer equipment, so maintain knowledge of your equipment and be able to remotely wipe it.
- Be cautious of E-mails Soliciting Donations FOR ANYTHING.
- Be cautious of e-mails and messages - Facebook /Twitter discussions - with links purporting to blog/discuss/show pictures of the latest person, place or thing.

Tips From The Trenches

How can you minimize the chance of becoming an Identity Theft victim?

- Don’t carry your Social Security card or any document(s) with your SSN on it.
- Don’t give a business your SSN just because they ask. Give it only when legitimately required.
- Protect your financial information.
- Check your credit report every 12 months.
- Secure personal information in your home.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches, and change passwords for Internet accounts.
- Don’t give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with.

Tips From The Trenches

- **NIST Guidance to combat Malware**
  - Develop and implement an approach to malware incident protection
  - Plan and implement an approach to incident prevention based on the most likely attack vectors
  - Ensure that your policies address prevention of malware incidents
  - Incorporate malware incident prevention and handling in your awareness programs
  - Implement awareness programs that include guidance to users on malware incident prevention
  - Maintain vulnerability mitigation capabilities to help prevent malware incidents
  - Document policy, processes and procedures to mitigate vulnerabilities that malware could exploit
  - Apply threat mitigation capabilities to assist in containing malware incidents
  - Perform threat mitigation to detect and stop malware before it can affect its target
  - Consider using defensive architecture methods to reduce the impact of malware incidents
  - Sustain a robust incident response process capability that addresses malware incident handling

What Can You Do?
And How Effective is It?

Acquiring security wares gets more complicated every day – there are currently some 1000 vendors offering more than 150 categories of products. Is it reasonable to expect that even the most well-intentioned person to know everything about what vulnerabilities they "fix" and how to use them. Still, **it is your responsibility** to make smart decisions about what to acquire and how to use them.

Note that even if you hire a managed security services provider or get antivirus/ antimalware apps you **can not** abdicate responsibility for what happens on your Network/on your Device. It has to be viewed as a partnership where **both work together** for optimum results.

Vendor (third party) data security polices and practices **must be** consistent with those of your company. Failure to make prompt disclosure of data breaches to affected individuals increases the risk of class action litigation.

Summary and Conclusions

Cyberfraud is one of the greatest threats facing the nation's economic future.

Everyone is in the front lines in terms of protecting their business and their family. They need to feel this and act in accordance with it.

5 – 10 years ago many people were fearful of technology. Today they are fearful of being without it. The fear of not being without your phone – nomophobia. Connections abound and are increasing – and each presents additional vulnerabilities and threats.

Everyone needs an understanding of how best to capitalize on your investments, manage relationships and achieve compliance with ever-increasing cyberspace rules, regulations and laws.

Knowledge of the risk environment enables you to minimize business and personal losses - lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity, lost money, lost credit, lost reputation.

Summary and Conclusions

Remember if it looks too good to be true, it probably is.

Knowledge and awareness, combined with appropriate technology, will protect you and your business/family.

Start using Risk-Based Decision Making, Fire Prevention rather than Fire Fighting