CYBER SECURITY

FOR YOU

WALTER L. TURNER

CYBER SECURITY

FOR YOU

WALTER L. TURNER

Cyber security can be very mysterious. The constant news about hacking can be very frightening. Either can leave you wondering if you will be the next victim. This book is for the majority of people who aren't involved in cyber security for a living. It's for those who do other things. It's an attempt to make cyber security simple, to acquaint you with the basics, and to provide you with easy things you can do to protect your family and your business from those who would use a computer to do you harm. Though terms will be introduced, no specialized knowledge in systems and network administration or IT security is presumed.

You might be a homeowner wanting to protect your family. You might be a small business wanting to know what you can do that is low cost, yet effective. You might be a CEO/CFO/COO/Board Member of a large enterprise wanting to communicate with your IT department more effectively about this most important subject. CIO/CISO's may also find this book helpful in educating corporate members on cyber security.

Cyber security is a global problem. This book is my attempt to move the ball forward.

Remember, forewarned is forearmed.

Dedicated to Andrea, my wife, who has the patience of Job.

Acknowledgements

This book is only possible because of the following people: Todd D. Lyle for showing it could be done; Michael Lentz for technical review and Mike Taylor for his helpful comments; Jon and Diane van Hoff for making it readable; and Linda Strother for publishing assistance.

Table of Contents

1.0 What is Cyber Security?

Computer and data security is broadly divided into physical security and logical security. Physical security (sometimes referred to as just “security”) includes building and personnel security. Logical security is focused on the data—both in storage and in transit on the network—and is sometimes called cyber security. Cyber comes from the word cybernetics which means the science of communications and automatic control systems. The military uses “cyber” to refer to computers or computer networking.

The general perception that cyber security is a relatively new field is false. Only the current emphasis in the media is new. Cyber security has existed for years; however, it previously received minimal funding and attention due to the costs of cyber defense. It also lacked visibility, because you don’t see attacks that were deflected—nor do organizations want you to be aware of how many times they have been attacked.

This book is a broad overview of cyber security. There are several sub-areas of cyber security, but not all experts classify cyber security the same way. There is not, as of yet, an agreed upon division or taxonomy of the subject. But, relax. This book does *not* cover all these sub-areas and their sub-areas in detail. There are just enough highlights to make you an informed consumer, employee, or manager.

Cyber security tends to employ military terms like defense in depth, target, attack, offensive, and defensive. The various areas of cyber security use lots of terms that may be foreign to you. Included at the back of this book is a glossary of terms.

The decision of a hacker (or the hacker's sponsor) to mount an attack is based on the perceived reward versus the risk—in other words, the ability to obtain or manipulate data without negative consequence. A defensive investment in cyber security—or how much you are willing to spend to defend against hacking—is driven by the value of the data versus the perceived risk of it being stolen, changed, or destroyed. As an example of low cost security, I used to have a large dog that accompanied me on trips. To create the illusion of high risk, I would leave a two inch chewed-through bone on the front porch while I was gone. It never failed to work.

So, what reward is worth the risk for a hacker?

1.1 The Hacker's Objectives

There are many reasons why people hack computer powered devices, but they all boil down to data. Steal data! Change data! Destroy data!

The motivations and objectives of hackers vary widely. Motivations range from idle curiosity to criminal intent. Perhaps the hacker just wants to brag that he or she can do it—proving one's cyber manhood (or womanhood). Perhaps the hacker was paid by a nation-state for political and military benefit. Maybe the hacker was hired as an industrial spy for competitive and personal gain.

Objectives can be as simple as proving that the hacker could "log in" or as complex as stealing information from someone's network for years without being noticed. Most of the time, the motivation has nothing to do with you personally, except that your data was valuable enough to merit the risk.

As examples, objectives might include:

- Denial of data access (blocking someone from accessing a storage device).
- Intellectual Property (IP) theft (stealing the top secret formula for a soft drink).
- Inflicting loss of reputation through exposure of sensitive information (revealing a political candidate's tax returns or medical records).
- Creating loss of trust in a corporation (exposing a bank or credit card institution's security weakness).
- Extortion (demanding a ransom payment in return for restoring one's data access or keeping sensitive data from becoming public).
- Kinetic effect (having something happen in the real world—such as shutting off a power grid, controlling a patient drug infusion device, or controlling an airplane).

1.2 Targets

The target is what the attack is directed against. The primary target is whatever the main objective is—think data, data, data. The intermediate target is the hacker's means to achieving the primary target. Intermediate targets include a network or network appliance, server, workstation, and mobile device (tablet, laptop, phone). Also included are infrastructure devices such as network connected thermostats, circuit boards, and the software applications that run them. Many different types of devices are now connected to the Internet and controlled using webpage based interfaces. These devices can be particularly susceptible targets unless proper investment is made to produce secure programming code.

Data is the end goal of attacking a target. Data can take many forms. A few examples are records in a database containing customer data or health records, data files such as word processing documents or drawings of intellectual property, your GPS location, the words being said in a conference room, your personal credit card information or that of your customers, and even video information.

1.3 Offensive

Think football. This is the other team. The one wanting your data or wanting to do damage to you. The offensive has different plays that it can run such as distributed denial of service (DDos) attacks, phishing and spear phishing, malware, social engineering, software and hardware flaws, and insider threat. We'll be calling the offensive "bad actors" or "hackers" throughout this book.

1.4 Defensive

You or your team (the home team, the good guys) need to stop the offensive, otherwise the bad actors will win. The defensive has tactics that can be used to prevent a cyber security breach:

- Training and education
- Policies and procedures
- Law enforcement agreements
- Information sharing
- Threat intelligence
- Counter intelligence
- Hardware and software
- Current patches and techniques to improve security
- Encrypted data and hard drives on anything mobile—those things that are easily lost or stolen, such as phones, tablets, and laptops

Some of these tactics are beyond the scope of this book, but many are covered herein.

1.5 Post Attack

After a successful attack, there is work to be done in the areas of forensics, legal, insurance (hopefully purchased before the attack), damage assessment, and target cleanup/validation. In addition, policies and defenses must be examined to figure out what went wrong and how to do a better job next time.

It might be hard to get motivated and started on your defensive measures, if you don’t know why cyber security matters. Read on!

2.0 Why Should I Care About Cyber Security?

Good cyber security is tedious and expensive. For businesses, though, the alternative is loss of customer good will and potential closing of the business. On the personal side, the inconvenience of identity theft, data loss, and invasion of privacy exact a heavy toll on your finances and your time. The result is an unfair burden on small businesses and individuals. It is important to recognize that this is the way it is, this is the world we live in, and accept a personal, even if limited, role in being a good data steward and protector. This chapter discusses a select few of the cyber security incidents of the last couple of years in various categories to help you understand the magnitude and variety of what's out there.

By being aware of the targets, potential attacks, and the defensive tools you have, you can diminish the hacker's perceived relative gain for the time spent on you. For example, if a hacker determined that the profit was only a few cents per hour for the time spent, the hacker would find something more lucrative to do. In time, if we (the defensive team, the good guys) diligently protect ourselves, the sheer number of hackers and attacks will be reduced. The rest of the battle will become easier to defend against and we might even be able to track down those few remaining bad actors.

2.1 Ransomware

Ransomware is software that encrypts all the contents of a hard drive and then extorts payment, usually in bitcoins, in order to get the unlock code. Some ransomware can even encrypt any attached backup drives. Ransomware can and has been used against many individuals and was recently used against several hospitals. The use of ransomware is a very lucrative area for the bad actors—the offensive team. Some bad actors have capitalized even more on their investments by running ransomware help desks. To pay or not to pay, that will be the dilemma when ransomware strikes you or your company.

2.2 Medical Records

Medical records are worth about ten times what credit card numbers are on the black market.[5] “Why?” you ask. Because medical records can be used to file fraudulent claims. It takes much longer to realize your medical records have been compromised than to notice a problem with your credit card number. This time differential combined with the relatively poor cyber security of hospitals provides hackers with a very lucrative market.

Note that medical records fall under HIPAA. HIPAA is the Health Insurance Portability and Accountability Act—you probably signed a form at your doctor’s office. Health providers are legally obligated to take reasonable steps to protect your healthcare information. Penalties are based on the level of negligence and can range from $100 to $50,000 per violation. This is capped at $1.5 million per year for violations of each HIPAA provision.

2.3 Human Resources (HR) Records

The largest HR or personnel records breach (break in with theft/manipulation of data) in history occurred in 2015 at the United States Office of Personnel Management or OPM for short.[11] The breach involved the theft of 21.5 million US government employee records along with 5.6 million fingerprint records. Keep in mind that these records contain the contents of the SF86—a questionnaire completed when applying for a security clearance—and include information not only about the applicant, but also about their extended families and neighbors. It is rumored that the Chinese are using the information from these records to put together a "Facebook" of US government and military personnel that can be used to put pressure against them or co-opt them.

This breach was a classic case of risk versus reward. Enough golden eggs (records) existed in one place with the potential for enough damage that they were highly sought after and justified the expenditure of almost any effort to obtain them.

Access was obtained through a breach of a US Government contractor who had access, and, unfortunately, less security to go through.[12] We—the defensive team, the good guys—failed to encrypt the records, disperse the records (so they're not all in one place), and keep non-current records offline. To make matters worse, the intrusion was not detected for a long period of time.

2.4 Customer Records

Target, the major retailer, was hacked on Black Friday in 2013. Over 40 million debit card accounts were scooped up. The data was not encrypted. Groups of Target customers filed suit claiming that “Target failed to implement and maintain reasonable security procedures and practices.”[13] Roll forward to 2015 when Target paid out $10 million to customers as a result of lawsuits. This $10 million does not include costs to notify, legal costs, loss of good will among existing customers, and the effect on Target’s reputation in the marketplace.

2.5 US Infrastructure

The chief of the NSA (National Security Agency), Admiral Michael Rogers, said that it is a matter of when, not if, a foreign nation-state launches a cyber attack on US critical infrastructure.[6] Critical infrastructure includes the electric grid, water, sewage, traffic, and more. Even dams can be hacked.

In December 2015 Ukraine suffered an electrical power blackout of 225,000 customers. The blackout was attributed to cyber attack via a Russian group. In March 2016 the US Justice Department indicted seven Iranian hackers. Among their targets was a small dam, the Bowman Avenue Dam in New York. If a gate had not been disconnected for maintenance, the hackers would have been able to manipulate it and flood part of Rye Brook, New York.

The US power grid has been hit with an average of one cyber or physical attack every four days between fiscal 2011 and 2014.[7] The Pentagon estimates that one major cyber attack on the electric grid could take weeks to fix.

Is your business such that you need power from more than one utility provider, as is often the case with data centers? Perhaps it would be wise to create another company location in another section of the power grid, where it would not likely be affected by a regional disruption. The unaffected location would be able to take over business should the need arise.

2.6 General Statistics

Some general cyber security statistics for 2015 that may be of interest to you or your company:

- 21.5 million records and 5.6 million fingerprints from the OPM breach[16]
- 1.9 million records compromised every day[16]
- 300 million records at online shopping site AliExpress[16]
- 707.5 million total data records compromised that were *reported*[16]
- 191 million US Voter Registration records compromised[17]
- 374 healthcare breaches[16]

Cyber criminals have raised their rates with the following rates for 2016:[14]

Corporate mailbox hack	$500
Private mailbox hack	$129
Credit card number	$ 7
Premium credit card number	$ 80

Origins of hacking attacks are many and varied. By country, here is the top seven list:[15]

China	41%
United States	10%
Turkey	5.6%
Russia	4.3%
Taiwan	3.7%
Brazil	3.3%

Romania	3.3%

In case you're curious, the US is a preferred place to hack from by many hacking groups due to the higher speed of the computers in general. Remember, the listed country source of the hack may not match the real origin of the hack due to IP spoofing or a computer being controlled from elsewhere.

And the final statistic—the one that really hits home: the average cost of a breach has grown to $4 million.[18]

Are you concerned about cyber security yet? Let's look at some specific ways that bad actors attack. First up, through email—something you might use every day!

3.0 Attacking Through Emails

Just about everyone uses email. It’s a convenient way to communicate, but can be a source of trouble. In this chapter we’ll discuss scams delivered by email, phishing (not fishing), and spear phishing as means of attacking through your emails.

3.1 Email Scams

Email scams are similar to phishing emails (discussed in **Section 3.2 Phishing**) in that the bad actors want something. Many times the email is sent to start a very personal correspondence or a series of calls. Picture a room full of people with computers. Their scam email has just been sent out. Within *minutes* someone shouts, “Got a live one!” and everyone snickers before the shouter begins talking to the person in a very sincere voice.

Think this doesn’t work? Nigerian email scams started 20 years ago. Now, note the date at the top of the following email showing when I received it. *If it did not work, they would stop doing it!*

The example below is a lazy one—the bad actors just want you to email your bank account number and personal identifying information to them. Many want you to call or write. Then they gradually hook you. All have a time frame when the wonderful offer will expire if you don’t act soon.

Note the official looking postscript at the bottom stating that the email has been scanned by Avast antivirus software. Ha-ha! Remember, if something is too good to be true, it probably is.

RE: INSTRUCTION TO TRANSFER OVER DUE PAYMENT OF $5.8M

From: Rev.Lee Johnson Add to Contacts
Sent: Mon, Apr 18, 2016 at 4:38 pm
To: Recipients

INTERNATIONAL FINANCE CORPORATION.
LEICESTER CURRENCY
CHEQUE/DRAFT DEPARTMENT
TELEGRAM: FBNFOREX

RE: INSTRUCTION TO TRANSFER OVER DUE PAYMENT OF $5.8M

ATTENTION:

This is to inform you that this office received payment advice from The Nigerian National Petroleum Corporation (NNPC) in conjunction with the Ministry of Finance of the Federal Republic of Nigeria to pay to you the total amount of US$5.8 Million. Note that a final approval has been given to your claim and your funds have been transferred from the International Finance Corporation World Bank Group which hasthe final authority to transfer out of the shores such amount of Fund.

We have just received an email from one MR. KAMICHI ***** who introduced himself as your next of kin also that you have instructed him to receive the funds into his account on your behalf. MR. KAMICHI ****** informed us that you are dead also that the instruction was given to him before your death. We have asked him to forward the copy of the letter you gave him but have not yet heard from him.

THIS IS THE ACCOUNT DETAILS HE FORWARDED TO US:
Bank Name: MIZUHO BANK, NARIMASU BRANCH.
Address: 2-11-2, NARIMASU, ITABASHI-KU, TOKYO, JAPAN
SWIFT CODE: MSDKBGHUT. Bank Account No: 239-1-563-321.
Beneficiary: ROS LTD. (KAMICHI BLAKE)

We are writing you to confirm this message and if it is not true, you are required with immediate effect notifying us of the need to rectify this fallacy. Please note that a government issued identification would be required to ascertain the authenticity of your claim.This office would also furnish you with details on how to obtain the transfer Authorization code which proves you the rightful beneficiary of this fund as we don't want the fund to get to the wrong hands. Since that is what our correspondent bank in USA needs for the transfer of your fund to your designated bank account.

We await your urgent response.
Rev. Lee Johnson

3.2 Phishing

Phishing emails are sent to all the email addresses the bad actors can get from buying lists or scraping emails off the web. The email *appears* to be from a company you recognize or have done business with and contains an issue or deal meant to move you to action. Links are provided, but they do not take you where you think you're going!

> **Bad Actor:** "We hope the potential victim does business with the place of business on the email. If not, there are lots of other ~~suckers~~ prospective victims just waiting for us."

I get lots of these, often several a day. I present you with some samples—minus, of course, the bad links. I have made images, so the links are not active in this book. Remember, these were *not* sent by the company they *appear* to be from.

The first sample (see image below) *appears* to be from LinkedIn. If the receiver of the email is a member of LinkedIn, that person will be interested. Note the "Important Message" warning in the subject line.

> **Victim:** "Dang! My profile has a situation. I'd better hurry and click, so I won't miss any of those messages I get from LinkedIn."

The mailing address at the bottom is a nice touch, don't you think?

Important message for walt_turner@SecureWebApps.com
From: Linkedin Support Add to Contacts
Sent: Wed, Apr 27, 2016 at 3:21 am
To: walt_turner@SecureWebApps.com

Good morning,

We found a situation on your profile today, please view complete message here.

This message is sent via HTML click here to view.

Thanks,
Bennett, Andrew
LinkedIn Corporation

LinkedIn Corporation, Mountain View, California, USA, and LinkedIn Ireland, Dublin, Ireland, October 23, 2014

OR BY MAIL at:

For Members in the United States:
LinkedIn Corporation
Attn: Agreement Matters (Legal)
2029 Stierlin Court
Mountain View CA 94043
USA

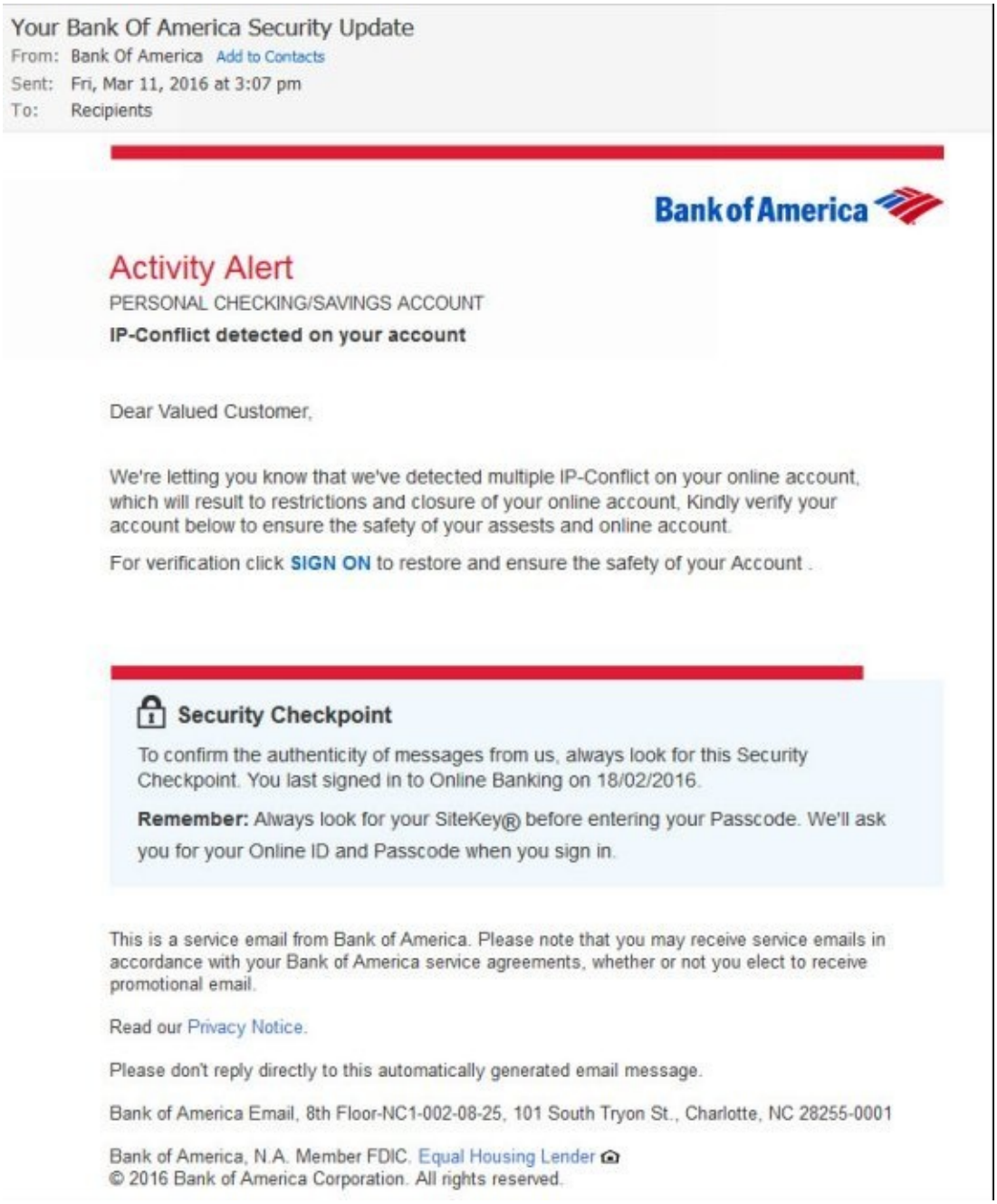
Coming up is one from Bank of America (BOA). It's pretty and has their logo and colors and looks very real. It even has a "Security Checkpoint" on it (whatever that is), so the receiver will believe it's real.

> **Victim:** "Oh, man! There's a multiple IP conflict on my account and they are going to close it. I don't know what a multiple IP conflict is, but I'd better act fast. Whew!"

A lot of thought and effort has been put into realistic looking details, including that BOA is an Equal Housing Lender—complete with a link to that site.

Oops! This is the United States and the date used in the Security Checkpoint is formatted

18/02 *not* 02/18. Still, not a bad job. The bad actors are hoping that, when it's mixed in with the 200 other business or personal emails you receive every day, you will *take action* without thinking.



Your Bank Of America Security Update
From: Bank Of America Add to Contacts
Sent: Fri, Mar 11, 2016 at 3:07 pm
To: Recipients

Bank of America

Activity Alert
PERSONAL CHECKING/SAVINGS ACCOUNT
IP-Conflict detected on your account

Dear Valued Customer,

We're letting you know that we've detected multiple IP-Conflict on your online account, which will result to restrictions and closure of your online account. Kindly verify your account below to ensure the safety of your assests and online account.

For verification click **SIGN ON** to restore and ensure the safety of your Account .

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint. You last signed in to Online Banking on 18/02/2016.

Remember: Always look for your SiteKey® before entering your Passcode. We'll ask you for your Online ID and Passcode when you sign in.

This is a service email from Bank of America. Please note that you may receive service emails in accordance with your Bank of America service agreements, whether or not you elect to receive promotional email.

Read our Privacy Notice.

Please don't reply directly to this automatically generated email message.

Bank of America Email, 8th Floor-NC1-002-08-25, 101 South Tryon St., Charlotte, NC 28255-0001

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2016 Bank of America Corporation. All rights reserved.

Ok, one more. This one *appears* to be from Chase Bank. This time I have "suspicious activity" on my account.

> **Victim:** "Oh, no! My account is suspended! How did … Oh, they tell me how it got suspended and all I have to do is click on this button to fix it. How thoughtful."

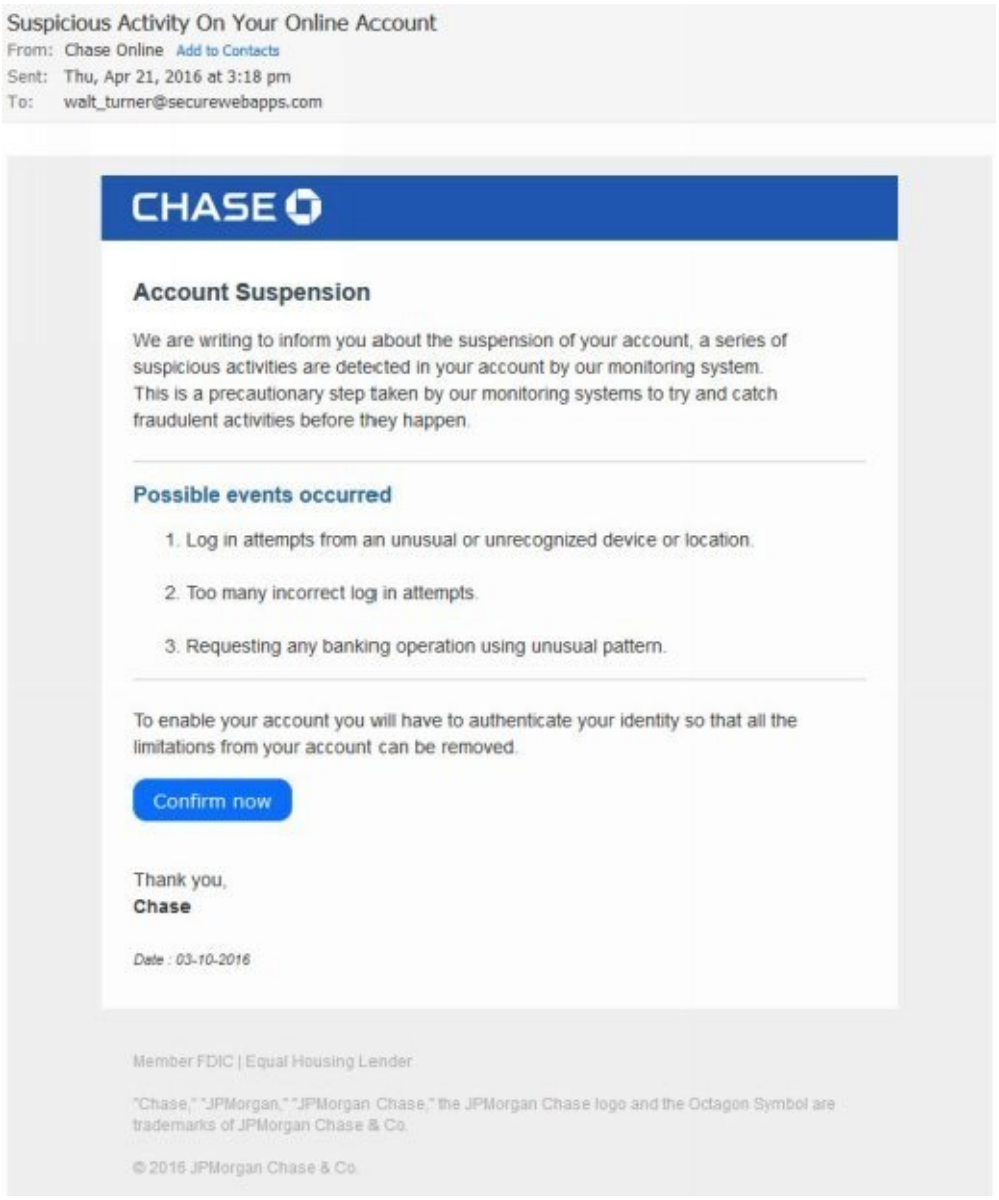
The button takes the victim to a website page that looks like a Chase Bank page—complete with logo.

Victim: "It says the bank is a member of FDIC, so it *must* be ok."

The victim is asked to verify the account by entering the associated login and password. Who has that information now?

Bad Actor: "By the time they figure out I got their password, I will have the real bank transfer funds from their accounts to my account in another bank that will only exist temporarily until I can cash out of it, with *their money*."

This phishing scam works because the victim is taken to a website page that *seems* legitimate—like www.chasebank.com—while the *real* bank is at www.chase.com.



Suspicious Activity On Your Online Account
From: Chase Online Add to Contacts
Sent: Thu, Apr 21, 2016 at 3:18 pm
To: walt_turner@securewebapps.com

CHASE

Account Suspension

We are writing to inform you about the suspension of your account, a series of suspicious activities are detected in your account by our monitoring system. This is a precautionary step taken by our monitoring systems to try and catch fraudulent activities before they happen.

Possible events occurred

1. Log in attempts from an unusual or unrecognized device or location.
2. Too many incorrect log in attempts.
3. Requesting any banking operation using unusual pattern.

To enable your account you will have to authenticate your identity so that all the limitations from your account can be removed.

Confirm now

Thank you,
Chase

Date : 03-10-2016

Defensive Tactics and Solutions

- Remember that no legitimate company ever asks you to click a link in an email and enter your login/password on a website.
- Pick up the phone and call and verify. Don’t use *any* number or other contact information on the suspicious email.
- Run the cursor over the link and carefully check the lower left corner of the browser to see if the URL is valid. Watch out for URL’s similar to the real one.
- Avoid opening attachments until you know the source of the email.
- Use a different email than your regular email to sign up for things on the Internet.
- Hire an outside firm to train and test your employees with a phishing campaign that records who responds to it. Follow up with training!

3.3 Spear Phishing

Spear phishing is simply targeted phishing. While phishing is more general—say, all Bank of America customers—spear phishing often targets a specific person or organization. For example, you receive an email with your company's email and name on it—complete with company logo—so it looks just like it came from someone in your organization, possibly your boss. And who wouldn't reset a boss's password and create another or lend one's own login if the boss were in a hurry?

> **Victim:** "Darn, the boss has forgotten his password again. That's three times this month!"
>
> **Real Victim - The Boss:** "You gave *who* my password?"

The spear phishing email could *appear* to be from a friend or loved one. Spear phishers attempt to make you drop your guard just a little bit. They may use information you post on Facebook or elsewhere to figure out what to put in the email. The email could reference a recent purchase you made—for example, iTunes—if your Facebook post shows you with an iPhone. Or how about a photo you posted two years ago with you and another person you tagged. The bad actor writes you and includes the photo with a comment like "those were some good times, huh?" The bad actor is trying to associate "shared memories" with you to gain your trust.

Defensive Tactics and Solutions

- Use a different internal email signature than you use outside the company.
- When you send an email with a link, include at least a minimal amount of text with it to ensure the receiver knows it's from you.
- Run the cursor over the link and carefully check the lower left of the browser to see if the URL is valid.
- Adopt a company policy to *never* ask for your login/password through an email.
- Have your friends use your middle initial or a nickname when they address you.
- Call the person who sent the email to verify the source is reliable before clicking on a link or opening an attachment.

Increasingly, a company's board of directors is the target of a spear phishing attack.[22] Or, the spear phishing could involve the transfer of funds from a company to the bad actor as

described in the next section.

3.4 Spear Phishing for a Fund Transfer Scam

There is a variation of spear phishing that goes like this. Suppose you are the person in charge of funds, say the CFO. While your CEO is on a trip, you get an email from her that may even sound like her directing you to wire some funds to an account—just as she is about to go into a meeting and she needs it sent *now*. What do you do?

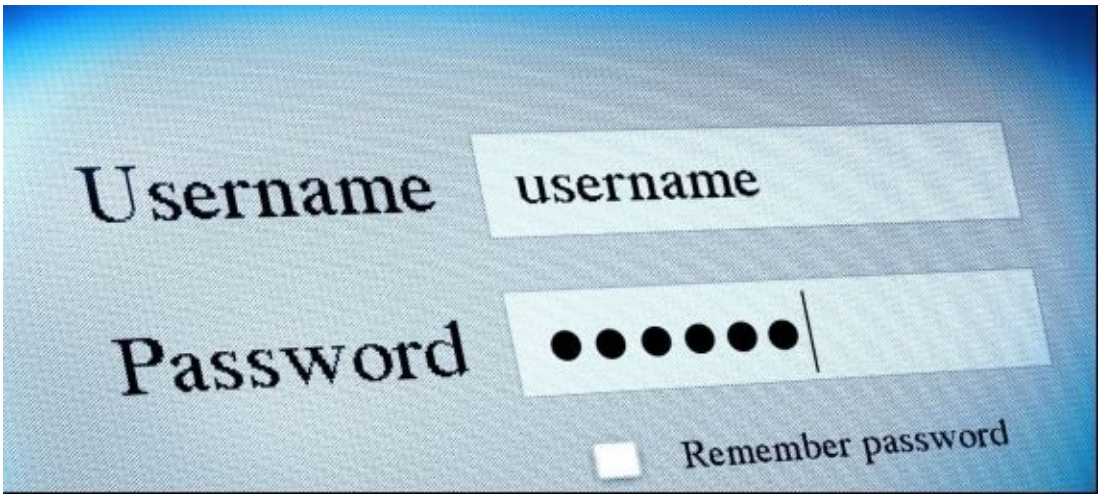
If you think spear phishing can't possibly work, think again. The FBI[1] reports that between 2013 and mid-2016 there were 12,000 reported company victims worldwide with $2 billion lost to this scheme. This was recently updated to over 22,000 victims and $3.1 billion lost.[24]

Defensive Tactics and Solutions

- Adopt a company policy that all fund transfers over $1000 must be verified by phone with the requesting individual.
- Adopt a company policy that prevents the CEO from authorizing fund transfers while on a trip.
- Create a place to request fund transfers after login to the network and only authorize certain individuals to do this.

We've just seen how giving your password to someone when you're asked for it can be dangerous, but the bad actors can also get it without asking for it! Read on to see how you can protect your password.

4.0 Attacking Though Passwords



Think your password is a good one? We shall see in this chapter.

4.1 Dictionary Attack

Lots of people use a dictionary word for a password. For example, **nebraska** or **hamburger**. These are easy for a computer to guess by running through the words in a dictionary and rapidly trying each as a password until a match is found. For a simple password this can take less than a second. If you take the same password and add a number and a special character such as **!**, it can take over 24 hours as it is no longer a dictionary lookup, but rather brute force (see **Section 4.2 Brute Force** below). Make your password a pass phrase like **overtherainbow** and it takes over 730 years.

4.2 Brute Force

Brute force is just that. Think of it as instead of picking the lock, the bad actor smashes through the door. This is done by trying all possible passwords until a match is found. Obviously, the longer the password and the greater the number of who possible characters to pick from, the harder it is to guess. That’s why many online accounts ask for combinations of uppercase and lowercase letters, numbers, and special characters with a minimum length.

4.3 Guessing

Little bits of information gathered about the victim make it easier to use cleverness in guessing the password. Lots of times people use their birth date or their children’s birth date or their address as all or part of their password. Or their Social Security Number or part of it and so on. This makes some passwords easy to guess.

4.4 Good and Bad Passwords

A good password is one that is hard to guess. Without going into the math behind the permutations, suffice it to say, longer is harder to crack. The more variety in characters, the harder as well. For example, if each character of a password can only be lower case letters, then in English there would be 26 possible values for *each character*. Add capital letters, and the number of possible values goes to 52. Add in numbers 0-9 and the possibilities are 62. Add in special characters such as **& * ( )** and the number of possible characters for *each character* in your password goes to 84. Requiring an uppercase letter, a number, and at least one special character makes a password much harder to crack.

People often forget that their username functions in a similar way to that of their password in that most must be guessed. Common usernames are “admin,” the first initial and last name, the last name and first initial, and email addresses. When the username is built like a password, for example, **D7bz#1Yh34!**, the complexity for the bad actor who is trying to determine your login is greatly multiplied. While it may be hard to remember the above username, any variation from the normal will make it harder to guess. If your last name is **Simple**, using the word **Complex** instead will throw off the bad actor.

4.5 Smart Password Usage

Let’s assume a login/password is compromised, meaning a bad actor has it. Was the same password used for multiple accounts? Uh-oh! Now the bad actor will try it on other accounts looking for a credit card on file.

> **Bad Actor:** “Let’s try Amazon and see if they have an account there with an active credit card. Summer is coming up and I need some outdoor gear.”

Defensive Tactics and Solutions

- Use one password for all accounts that don’t have an associated credit card.
- Use a different password for each account with a credit card. If one account is compromised, the others should remain safe.
- Use a strong password on the accounts with a credit card.
- Unless you use an account every day to make purchases, don’t attach or save a credit card—instead enter the card information at checkout.

4.6 Password Do's and Don'ts

Creating strong passwords—and usernames—isn't difficult. The following guidelines of what to do and what not to do should help:

- Don't use a family name or birthday as a password.
- Don't use the family pet name or your favorite sports team as a password.
- Don't use a banking PIN as a password.
- Don't use a password so complex that it requires a yellow sticky note on your screen to remember it.
- Don't use a dictionary word as a password.
- Don't share a password. If a password is shared, change it afterwards.
- Don't pick a username associated with meaningful information, such as name, address, and so on. Remember, the username works just like a password in that it, too, must be guessed.
- Do use a password wallet like RoboForm™. They are safer than letting your browser store your password.
- Do change a password at least every six months. Change it earlier if you suspect or are notified of trouble with an account or a breach at the place the account is.
- Do use a password phrase that can be remembered, such as **snow7beach14!** But, *do not* use numbers that are meaningful, for example, ages (kids are 7 and 14), birthday (July 14), or house number (714).
- Do use a long password of at least 12 characters, if possible. (The one just above in bold is 13 characters in length.)

Your username and password are strong and secure now. But what about your connection to the world?

5.0 Anatomy of a Simple External Attack

Let’s now talk about an external attack against a system. There are many ways to attack from outside a computer system. This section describes a simplified version of just one way to attack.

5.1 Step 1: IP Scan

Hacker tools begin by scanning a range of IP addresses looking for a system to hack. The tool sends a PING command and the device on the system responds back. This is how the hacker knows the device exists. Then the hacker determines if it *can* be hacked and whether there is any value in hacking it.

5.2 Step 2: Port Scan

Once a target system is found using IP scans, a port scan is undertaken to determine ports that are open. Ports are used to communicate to and from the outside world. Each computer has over 65,000 possible ports with few actually used. Each port is generally assigned a particular application. For example, a web server listens on port 80, unless it’s using SSL or TLS, and then port 443 is used. From the default ports, the hacker can develop a list of applications on the computer and based on knowledge of the applications, can send commands to cause the applications to reveal their version numbers—and that can lead to knowing version weaknesses.

5.3 Step 3: Known Vulnerabilities

Each standard application in use on the Internet has known bugs with each version. The hacker is looking for an application that hasn't been kept up-to-date with patches to those bugs. Once an application to exploit has been found, the hacker can utilize that vulnerability to gain access to the computer. Once *one* system is compromised, the hacker can move laterally in the network to gain access to the next computer.

In the event no hackable application can be found, the bad actor moves on to the next system or finds another way in, such as phishing or social engineering (see **Section 7.0 Attacking Through Social Engineering**).

You might not have a "system" to be attacked, but you most likely have several *things* connected to the Internet. Each of these is vulnerable as well.

6.0 Attacking Through the Internet of Things

The Internet of Things or IoT is the attachment of physical objects, devices, vehicles, and buildings to the Internet either though a hard-wired connection or through Wi-Fi. A single item on the IoT is known as a *thing*. It is projected that the IoT will, in time, consist of billions of *things.* In this chapter, we will examine some of those things and their roles as attack paths or vectors for hacking.

6.1 Video Cameras

Most computers these days are equipped with a webcam which means video and audio. Add a little malware and your own camera can spy on you at the behest of someone half a world away. The talented hacker can even do it without the camera's red light coming on. A bad actor can buy a Blackshades hacking kit for $40 (estimated sales between 2010 and 2014 of $350,000) and start listening and looking in on you. Why, oh, why, don't the manufacturers put a physical OFF switch on these things?

Think it can't happen to you? Do you own a home security system equipped with a webcam? How about a video baby monitor that is Internet enabled? Go to the site shodan.io. There you will find 6,940 unprotected webcams, which means webcams without a password or ones still set to the factory setting for a password.

Defensive Tactics and Solutions

- Unplug your video camera when you are not using it or cover the lens with a yellow sticky.
- Reset the login/password on your webcam. Contact the manufacturer to learn how.

6.2 Cell Phone Fingerprint Reader

Most newer phones have a fingerprint reader. It makes logging in much faster and offers some protections. However, if your fingerprint is on file in any government database, it might not be so safe. It is possible for a bad actor to 3D print your fingerprint and use the rubber version to fool your phone. Another downside of using your fingerprint for ID is that you can't change it! When a hacker takes your credit card number, you change it. When a hacker takes the digital version of your fingerprint, you are done using it for ID.[9]

Defensive Tactics and Solutions

- Use the fingerprint reader *and* a login for access.

6.3 Medical Sensors

Many wonderful devices will be forthcoming to aid in tracking your medical condition and reporting the results live to you, a monitoring facility, your doctor, and perhaps even your insurance company. This data will inevitably be stored somewhere and will be susceptible to hacking. Do you want your future hiring company to know you have an irregular heartbeat?

6.4 Wearables

Wearables can have a number of different functions. A wearable could have a medical sensor such as described above. It could be an aid to help you with your health goals or running goals. Smart watches, smart glasses, even high tech headphones qualify as *things* in the IoT. Remember, if it can be connected to the Internet, it can be hacked. Eight of the top ten wearables in 2015 did not have the capability of setting up a password—even your child could hack that.

6.5 Appliances

Won’t it be wonderful when your refrigerator can send a list of what you are out of to your store where your groceries will then be made ready for pickup? You can probably think of many communication-enabled appliances that would be nice. A bad actor has already been able to hack an Internet-connected TV and gain access to the home network—and thus to all the home computers and hard drives.

6.6 Automobiles

Automobiles are discovering the value of being connected to the Internet. But, because manufacturers use a single network throughout the car and cyber security is not the first concern, cars are vulnerable to hacking. Hackers, in one example, were able to take over the car's air conditioning, radio, windshield wipers, digital display, and transmission. This was a controlled test using a Jeep(R), but other brands have vulnerabilities as well. Hackers also claim the ability to kill the engine, cut the brakes, take over steering at low speeds, and track the vehicle.[30] Controlling any number of these components remotely could distract you into a wreck or could cause a possibly fatal accident.

Jeep is a registered trademark of Chrysler and also Fiat, Chrysler's owner.

6.7 Summary

What to do?

That’s difficult to answer, because the *things* connected to the IoT can and will vary so widely. This will be a general answer that may not fit every IoT thing.

Think about the data collected or what the *thing* is connected to. Think about the *thing’s* security and what the risks are if it is breached. Stay informed by watching the news for issues around the *thing* you are using. If it hasn’t been already, your *thing* will soon be given a security review and a write up or report. Think about the potential downside of a breach. Remember, the bad actors have automated tools, so the cost of going after your data is very little to them.

If you are a public figure, a government or military official, or a celebrity, your risk is higher than the norm for an IoT breach. You may want to have a cyber security expert consult with you regarding your individual circumstances.

This chapter has been about interaction with *things*. On now to our interactions with each other through *things* or with information gleaned from our *things*.

7.0 Attacking Through Social Engineering

7.1 Face to Face

For this one, let's do an imaginary conversation in a bar between the Cute Bad Actor (female) who is 20-something and the Defense Contractor System Administrator (male victim). Cute Bad Actor has already done her homework on the web to find her target for the night.

> **Cute Bad Actor**: "Hi, good looking! Anyone sitting here?"
>
> **Victim**: "Er, ahh, no."
>
> **Cute Bad Actor:** *Small talk questions and comments.*
>
> **Victim**: *Small talk answers. Excited at the interest.*
>
> **Cute Bad Actor**: "So, what do you do for a living?" *She already knows.*
>
> **Victim**: "I'm a system administrator, in fact, I'm over several administrators."
>
> **Cute Bad Actor**: "Uh, what's a system administrator?" *She already knows.*

… 40 minutes later

> **Victim**: "So, that's how I protect our networks! Pretty clever, huh?"
>
> **Cute Bad Actor**: "Wow, I'm impressed. And me, I'm just a simple file clerk." *Gotcha!*
>
> **Note:** This is not intended to malign all system administrators or to imply that they are all male or that all bad actors are female.

Not all the information may be collected in a single visit. It may take multiple visits to win the victim's trust. Remember the stakes are high, so time can be expended to get the information.

7.2 Telephone

Sexy-Voiced Bad Actor calls Support Tech Victim on her disposable cell phone after researching the company on the web to find the perfect position to imitate. She is hoping to get a male tech support person and may call back more than once to get one.

Victim: "Tech support. How can I help you?"

Sexy-Voiced Bad Actor: "Hi! This is Doris in Accounting. I forgot my password again."

Victim: "You aren't supposed to do that."

Sexy-Voiced Bad Actor: "I know, I'm just so dumb. **crying** Can you help me, please? Mr. Simmons is going to kill me, if I don't get this report out!"

Victim: "Well, I'm not supposed to …"

Sexy-Voiced Bad Actor: "Please? I will owe you a big favor, if you could just help me this one time."

Victim: "Ok. What's your login?"

Sexy-Voiced Bad Actor: "You mean my email?"

Victim: "Doris, you know we use your first initial and last name."

Sexy-Voiced Bad Actor: "I'm so dumb. I have trouble remembering anything that isn't a number. Guess that's why I chose accounting. **giggles** Ok. It's dswanson."

Victim: "Ok. I reset your password to **niceguy14**."

Sexy-Voiced Bad Actor: "Oh, you *are* so nice! … I'm in!" *He-he!*

Note: This is not meant to imply anything about tech support, only that this is one

of many ways social engineering is done by telephone.

A variation of this is that “tech support” contacts you at work or at home about a problem on your computer and convinces you to download a “scanner” to fix your problems which gives the “tech support” bad actor access to your computer. Another is a caller posing as your Internet Service Provider (ISP).

7.3 Facebook

A bad actor can use Facebook to learn more about a potential victim, if the profile is not private. The bad actor might be able to become friends with you and then view all your posts (not to mention photos, likes, and personal details) and all your friends' posts. Or maybe just your friend's profile is public, so at a minimum all *your* interactions with that friend are exposed. Somewhere in there, someone is careless and starts tagging photos with names or talking about an upcoming trip.

> **Bad Actor**: "Looky there! Bill is going to Hawaii with his whole family and he was ~~dumb~~ kind enough to post the dates he will be out of town. Time enough for me to physically slip into his house and put some malware on his personal computer. He mentioned on Facebook working from home. I'll get his company login info next time he logs in. Sweet!"

One hacker claims to be able to crack the Facebook security, view posts, and glean enough information to ruin you, should he desire. You can read more at this link:

http://www.theregister.co.uk/2016/07/20/silver_tongue_hacker_shows_how_one_home_ad

7.4 LinkedIn

LinkedIn allows a person from anywhere in the world to post an online resume. Since a goodly percentage of people on LinkedIn are looking for jobs, this can be taken advantage of by the bad actor.

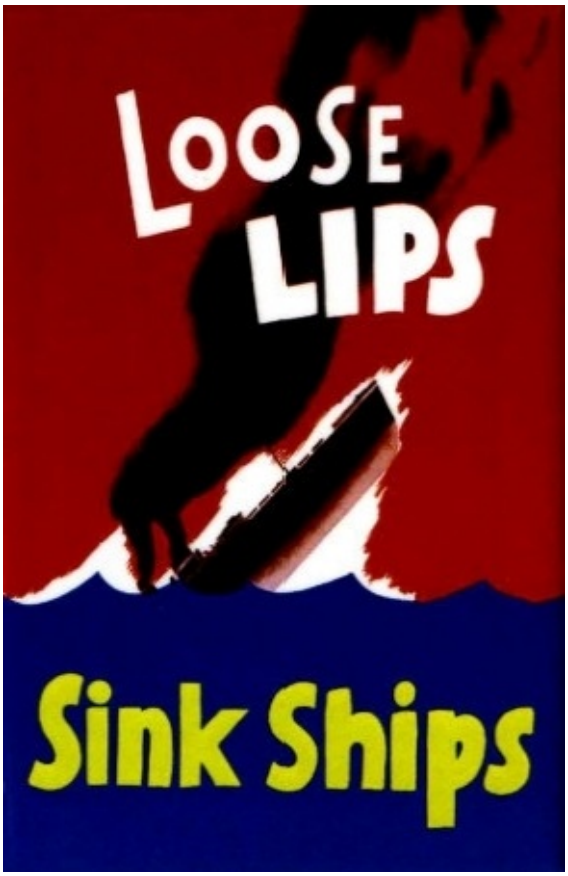
> **Bad Actor:** "Good! My recruiter profile is all done and I have found a handsome guy's picture to use. Let's see, here is a gal who works in the nuclear industry. I'll start a dialog with her and ask for her resume. After that I will call her and make her a job offer and get her to fill out some forms I send her. (*She'll never realize the forms have attached malware.*) I'll be able to take over her computer. Who knows … maybe I'll finally get to play with a reactor!!"

As a LinkedIn user, you can turn off access to the names of all your connections, not already in common, from viewers. This prevents the bad actor from pretending to know you with the intent of gaining a connection to your connections.

> **Bad Actor:** "Hi, Bob! I noticed that you and Joe Barnes are connected. Joe and I went to high school together in Sarasota (*location taken from your profile*) and I thought it might be good for us to connect as well."

7.5 Employees

Back in World War II, there was a slogan that appeared on posters in British factories. The slogan stated “loose lips sink ships”—referring to the damage one person who was not careful about what was said could do.



An employee in Area A befriends an employee in Area B and gradually learns her and Area B’s procedures. He gets a friend to invite her to lunch and manages to be at her desk before her login times out. He inserts a flash drive and copies malware to her computer. Now he can log back in from another computer and start paying invoices—invoices from his bogus company which will conveniently go out of business as soon as those nice checks are cashed.

Adult social and work interactions provide many opportunities for the bad actors. The bad actors are not above targeting those closer to home—our families—and those who can be most vulnerable—our children.

8.0 Family Safety

In this chapter, we’ll talk about things you can do to protect yourself and your loved ones from the bad actors.

8.1 Cell Phones

Cell phone applications (or apps as they are called) are software programs designed to work on your cell phone. Cell phone apps are distinguished from web apps, which require a browser to run. Cell phone applications have all the possible security flaws of traditional applications in that the user downloading the application often doesn't know the company and what the application is really doing, especially "behind the scenes."

Some applications have been known to listen into conversations, even when the phone is off and for as long as the phone has power.

The storage of the data for an app is often off the phone and is provided by the vendor of the application as a part of the cost of the application. This off-the-phone data storage puts your data outside your control. You don't know the levels of cyber security applied to your data. If your off-the-phone data is hacked, it could be used against you.

"How?" you ask. Suppose someone wants to know your location and any one of at least 13 apps your child has downloaded transmits GPS data even when the app is "off." If a hacker can identify you from the off-the-phone data, your location can be tracked when you have your cell phone with you. The hacker can determine if you have your cell phone with you by getting the GPS location of your home and then seeing if the GPS location transmitted by the application is different. You can extrapolate scenarios from this where the bad actor uses this information to rob your home, kidnap a family member, set up a robbery, or worse.

What to do?

Purchase a cell phone anti-tracking, anti-spying RFID signal blocker case or bag. That might sound like a terribly expensive item, but one of the popular sites for purchases has them listed for $9.95. When not using your phone, slip it into one of these bags. It has the added advantage that you won't get interrupted by your phone while it's in the bag, because it can't receive or transmit. Test your bag or case to see if it works by trying to call your cell phone.

If you don't want to go the bag route, limit the applications that you give access to your location (GPS position).

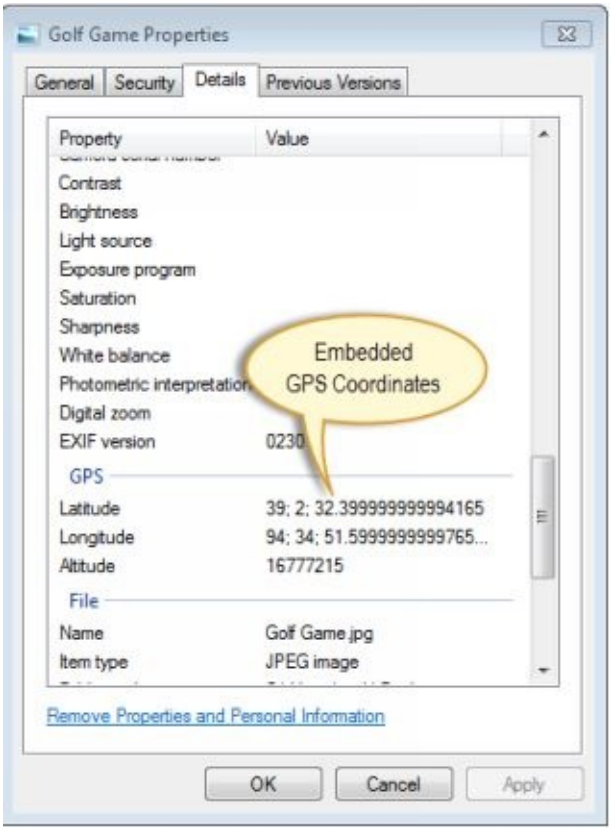
- Control the apps installed on your phone and do some research first.
- Don’t give an app access to your GPS information unless it’s a mapping app.
- Buy a bag for your phone to block transmissions when you are not using it.
- Check out the new phone from BlackBerry (DTEK50) that monitors all apps and transmissions to and from the phone. [32]

Another tangential problem is geotagging. Unless you have locations on your phone specifically off, your phone camera will geotag photos with the location where they were taken. A bad actor can access your online photos and determine where they were taken. If you take photos on a trip, the bad actor will know you aren’t home. If you take photos on a date, the bad actor will know where you are physically. If your children take photos, the bad actor will know where they go (or even where they are within your home).

Defensive Tactics and Solutions

- You can use a program to remove the geocoding from photos you post online. (See below for more details.)
- Don’t post trip photos until you are back home.
- Control your privacy settings and limit who can view the photos you post online.

To find a program to remove the geocoding from photos you post online, search for “exif editor.” EXIF is the encoding standard. It might be possible to prevent the geocoding from your phone itself, but this will vary by phone, model, and even the app used for the photo taking. You can easily, however, check if a photo or image has geocoding before posting it online by right clicking on the image (on Windows) and checking the properties tag as shown in this sample.



Yet another problem is the beginnings of ransomware on mobile phones. (For a review of ransomware, see **Section 2.1 Ransomware**.) The number of ransomware cases involving mobile phones reported by one source is up from 35,000 users affected in 2015 to 136,000 in 2016.[19]

Defensive Tactics and Solutions

- Do buy enough cloud space from your phone vendor to keep all your contact information backed up to protect against ransomware.
- Frequently plug your phone into your desktop and download a copy of your photos.
- Keep a copy of all your music on your desktop.

Finally, the bad actors are now using keyloggers on cell phones which are inserted through malware. This gives them the ability to record your login information and send it elsewhere.

Defensive Tactics and Solutions

- Don’t use your mobile device to log into applications containing sensitive data, especially online banking.
- If you feel you must log in, change your password when you get home, using your desktop.

8.2 Routers & Wi-Fi

These days, the router and Wi-Fi are combined into a neat little device that comes with your cable or Internet service. Did you know that the password is factory preset and thus knowable to the bad actors? Since each device has its own way of changing the password, simply do an Internet search on the make and model of your device for specific instructions. If your router can be compromised, it is possible to intrude into your home network.

Some steps to make your router more secure:

- Always use WPA2 and not the less secure WEP.
- Turn off SSID broadcast. If you prefer not to turn it off, at least change the SSID—the default usually gives away the manufacturer which helps the bad actor look for flaws.
- If you can, turn down your wireless radio to confine it to within your home.
- Turn on MAC filtering, so only devices whose MAC you have entered can connect to your network.
- If your router has a feature for remote management, turn it off.
- Turn off the router ping response.
- Change the default password.
- If your router has a DMZ feature, make sure it is turned off.
- Limit the size of your DHCP pool to the number of your devices connected to your network.
- WPA2 security is *not* foolproof, so adding some of these other measures *is* needed.[3]

If you need help with any of these settings or want additional resources about router and Wi-Fi security, check out this information from the FCC:
https://www.fcc.gov/consumers/guides/protecting-your-wireless-network

8.3 Computers & Tablets

The absolute minimum protection needed for a computer or tablet is a virus checker. You may wish to consider one that flags known bad sites. This will protect your device from all viruses except zero day viruses, which are rarely deployed against individuals (unless you hold a position at work that would make compromising your home computer an aid in perpetrating a breach at your work).

If you want more than that, here are some other tools:

Adware Checker

Adware checkers are handy programs that keep ads from popping up in your browser. Some sites detect adware checkers and don't allow entry unless you enter a bypass for that site, thereby allowing the ads while you are on that site. (The bypass is referred to as white listing.) Recently, some sites that required the visitor to white list them on ad blockers were, in fact, serving up malware with their ads.[25]

Browser Anonymity

Browser anonymity usually refers to plug-ins that prevent websites from reporting your use of that website to the often many trackers that watch your website browsing habits in order to vend you customized ads. The use of browser anonymity prevents third parties from monitoring where you visit on the web.

Not Falling for Their Tricks

Bad actors will try to trick you into downloading their code onto your computer and then running it. Here are just a few of the ways they do this:

- A website prompts you to download a (bogus) Active-X control.
- An advertisement mimics the download link of your browser.
- A box pops up saying you need a special plug-in to watch a video.
- A box pops up saying your computer is infected. The bad actor provides you with a simple solution. Click here to fix it!

This is, of course, not an exhaustive list, since the bad actors are always dreaming up new tricks and methods. The best protection is to be questioning. Why do I need that? Am I clicking the right button? Is that really required? Do I need to watch this video or will another do?

8.4 Email

Bad actors use email as a vehicle to get you to click a bad link or open an attachment capable of attacking your computer. The people in your family most likely to get a computer infected this way are children. Children tend to click on everything and get their computers infected. Once that happens, malware can send you an infected email in your child's (or grandchild's or niece's or nephew's) name. Do you click on links your family members send you? Or open attachments without running a virus checker against them?

Your family would not deliberately try to harm your computer, but people tend to trust emails from family members and don't think as much about cyber security when opening them.

8.5 Internet Access

Not all members of your family need Internet access. Not all members need access 24x7. Limiting access is a way to prevent access to “things not desired”—which often have malware associated with them. You can go high tech with products such as WebWatcher™ or Net Nanny® or low tech like us and take the power cord away at bedtime. Another good solution is to require that all computing devices (computers, cellphones, tablets) with Internet access be used in public home areas without the ability to take Internet accessible devices to private locations in the home.

8.6 Appliances

Appliances can be used to hack into your network. Consider the new TV or refrigerator that has Internet access—if it’s not secure, it’s an open doorway into your network. One solution is to use a dual channel router and put your appliances on a separate network from your computers or devices that contain data you don’t want stolen.

Remember, too, that a device that’s collecting information about you or your home—and storing it either online or in the device—is susceptible to hacking. The device could be your home security, your heating and air conditioning, your home lighting, and so on. Think about what information will cause you risk if it is stolen or manipulated. Got a fancy electronic lock system? Consider putting a key lock on one door and hiding the key just in case.

8.7 Special Risks for Children on Computers

Due to the innocence of children, computers carry some special risks:

Recruitment

Gangs, as well as ISIL (ISIS, Daesh), are recruiting online in a big way.

Grooming

Pedophiles and others can become your child's secret friend with bad possibilities following.

Cyber Bullying and Cyber Harassment

Cyber bullying and harassment are against the law, as is the more serious cyber stalking. If you think your child is a victim, start making screen snapshots and change your child's sharing permissions.[20] (The reference noted for the previous sentence is a very good source of more information about cyber bullying, harassment, and stalking.)

Cyber Stalking

Cyber stalking is similar to cyber harassment, but is the more serious of the two. It is characterized by the relentless pursuit of the victim using digital means. It could lead to a physical attack when the victim's location is known.[20]

Sexting and Revenge Porn

Sexting is the sending of a sexually provocative photo of oneself to another. A child involved in this can be charged under the existing child porn laws. Revenge porn usually occurs during a breakup when those sexually provocative photos get shared all over the Internet as a form of revenge. This has led some victims to the point of suicide.[21] (The reference noted for the previous sentence is a very good source of more information about revenge porn.)

Disclosure

Children don't know the ramifications of disclosing information online about themselves or their location like adults do. Children will also tend to disclose information about their parents. Most people don't need to know much about mom and dad—especially information such as when they are typically not home, whether they keep money at home, whether they have a gun, and so on. Children should be taught not to answer questions about their parents, but to turn those questions over to mom or dad.

Clicking on Links

Links can be made very enticing for children to click on. Not all links should be clicked on!

Downloading Applications

Lots of kids love to download games. Some games are the source of malware.

Pornography

Pornography is pervasive and children swap access information at school. It is addictive and your child may need help to stop viewing it. It is a problem not limited to boys. Pornography sites are also known for their malware.

Flash Drives

The bad actor leaves a bright-colored flash drive laying around. The child brings it (a free flash drive!) home and plugs it into your home computer not knowing it contains malware. Voila! This works with adults, as well.

Defensive Tactics and Solutions

- Keep all computers out of children's rooms. This includes cell phones and tablets, because they are small computers.
- Keep all computer screens facing in a direction so they can be viewed by others.
- Consider an application to limit children's access until you are sure they can handle the freedom.
- Switch your computer to a Linux-based operating system which will give you more control over it.
- Have an age-appropriate discussion with your children before turning them loose on the computer.
- Check the history log frequently on the browser. A good rule is that "if the history is missing, then it is assumed the contents were bad." Let your kids know that up front.
- Lock down children's social media to limit the exposure of their posts.

- Does your child need a cell phone? If so, consider limiting access to only apps you download and approve.
- Require access to all your child’s passwords for desktop and mobile devices and do random audits.

8.8 Social Media and You

Post Once, Remember Forever

Remember, once posted, it can't be deleted. Your posts and especially your photos can gain a life of their own through others reposting them across the Internet, so millions of people can see them. Remember that a "fun" post may not seem so "fun" when viewed by the potential hiring manager.

Imposter Accounts

An imposter account is one in which someone claims to be someone else. It's easily done—copy the person's photo and some personal facts and set up a social media account in the person's name. I was once contacted by a four-star general for a LinkedIn connection. Not having that many four-star generals ask to connect with me, it was fairly easy to detect that this was an imposter account. I took the extra step of contacting the Air Force to report the imposter in order to protect the next person.

Unofficial Presences

Bad actors also mimic the official social media presence of organizations. If you are in doubt, search for the organization and go to its official website. The organization's social media links are usually listed. Follow *those* links to get to the official presence.

Identity Theft

Identity theft involves the bad actor impersonating you when applying for credit. The bad actor might even apply for an identity card in your name with the bad actor's photo. As you can imagine, if someone else is you, it's difficult to prove that *you* are you. Cleaning up the mess can take hundreds of frustrating hours. The bad actor looks for key information such as name, date of birth, social security number, and banking information. The bad actor will try to piece this together from all your social media and other online posts. Beware of what information you are sharing.

Defensive Tactics and Solutions

- Be aware of your privacy settings, so you don't post private information to the world.
- Consider what your friends and family post online about you and your personal activities and details. They might be inadvertently sharing your information with the world.
- Invest in identity theft insurance, especially the kind that rebuilds your identity at the insurance company's expense and time. We use and recommend ID Shield™, although

there are many other alternatives.

ID Shield is a trademark of Legal Shield.

Moving on now from your family’s cyber safety, we’ll discuss company safety.

9.0 Company Safety

This chapter is about what you can do to keep your company safe, both as an employee and as an owner or president.

9.1 Insider Threat

An insider threat is the threat posed by an employee, contractor, or other person who has access to a company's information and systems. This *insider access* can be used to wittingly or unwittingly harm the company's interests through sabotage, unauthorized disclosure, data modification, espionage, or terrorism. This section will focus on the items in the above list as they relate to cyber systems and capabilities of your company.

Insider threats can have many indicators. In the spirit of equal opportunity, the following indicator examples will use he/his and she/her alternately:

Working Odd Hours: Working hours that are not the norm for him or others in his area.

Unauthorized Removal: Taking sensitive documents home or taking more documents than would be the norm for her area of work. Another indicator could be a sudden change in what is being taken home.

Seeking Info: Making inquiries of coworkers or other departments for sensitive information he would not be expected to need in the performance of his job.

Unauthorized Devices: "Mistakenly" bringing items such as smart phones, USB devices, or her own computer into areas of the company where these items are prohibited.

No Need to Know: Taking documents or files from areas of the company or from computer servers that he isn't reasonably expected to access in the course of doing his job.

Foreign Travel: Taking unexpected, unexplained, or unreported foreign travel.

Unreported Contacts: Having continuing contacts with foreign nationals or foreign governments.

Bragging: Talking excessively about work and what he knows when in mixed company.

Disgruntlement: Displaying signs of increasing dissatisfaction with supervisor, employer, or job.

Unexplained Affluence: Making purchases that seem to be "beyond her means."

Unnecessary Copying: Making excessive copies or burning lots of CD's.

Remember, a single indicator does not an insider threat make. If you think you have an insider threat, any of the US Intelligence agencies are willing to help or, if it involves foreign entanglements, to steer you to the correct agency. The FBI will also serve as a point of contact. If you are a defense contractor, you should already have a point of contact for counter intelligence.

Before I close out **Insider Threat**, let me tell you about a new device that helps in acquiring passwords. It's about the size of a USB storage device and can be used to harvest passwords from certain wireless keyboards *without ever touching the target*

computer, though it will need to be in the vicinity. Certain models are camouflaged to look like a device charger plugged into the wall.

There is also a new malware that activates home webcams and then, if compromising pictures are taken, the owner of the webcam (one of your employees) is blackmailed into being a threat to your business. [31]

Both of these last paragraphs were added after the book was done, but not yet published. This is a good example of how quickly new threats are developing.

9.2 Employee Training

By far, the vast majority of breaches can be traced back to something an employee did or didn't do[10], with employees being at fault in 25% to 90% of the breaches, depending on which article you read.

This suggests that one method of fighting breaches is to educate your employees. "What to educate them about?" you ask. Basic cyber security about passwords and phishing would be a good start. You could even ask them to read this book.

Also, talk to them about social networking sites. The more information they post about themselves, the easier it is for someone to impersonate them on the phone or in an email.

Employees involved in cyber security will need at least annual training due to the ever changing threats. Those who earn and hold cyber security certificates can help protect your company from potentially damaging breaches. Rewarding newly certified employees with a salary increase or bonus is considered minimal. Contact the FBI or a US intelligence agency for help with insider threat training.

9.3 Visual Hacking

Visual hacking is the reading of passwords or other critical information from over someone's shoulder. In a test performed in 2016, researchers were successful in doing this in 91% of the cases[33]. Protection from visual hacking includes moving away from the open floor plan, screen filters to limit viewing, and employee training. Unless invited to do so, it's *not* ok to look over the shoulder of someone logging in or to look at someone's screen.

9.4 Penetration Testing

Penetration testing is a service that will attempt to hack your software, servers, network, and other devices *for* you. It is invaluable in helping you determine if the cyber security measures your company has in place are adequate. It will also illuminate weaknesses, so you know where to shore up your defenses.

Ask around to find a company who is good at this. Several companies offer monthly testing of your defenses and provide you with a certificate of what they have done. This, too, is invaluable. See **Chapter 10.0 Reducing the Liability at Your Company** for more about this.

9.5 Think Cyber Security

The best cyber security comes from a work culture where cyber security is thought about and practiced by *all* employees, not just the ones in IT. Anyone can click on a link, visit a malicious website, slip in a flash drive they found in the parking lot, or take confidential records home or put them on their personal laptop. Anyone can *also* report an insider threat, spot phishing emails, run virus checkers on new files, and avoid clicking links or giving out your login/password. It’s all a matter of proper training and culture. We’re all in this together. A breach affects profits, which can affect bonuses and salaries, and possibly even job security.

9.6 NIST Cyber Security Framework

The NIST Cyber Security Framework is a document published by NIST (National Institute of Standards and Technology) that details suggested cyber security standards for businesses. It can be found on the NIST website: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

The document is all about starting where you are and taking the next step for your company. It's divided into five sections: Identify, Protect, Detect, Respond, and Recover. These sections are then divided into subareas with suggestions for each, including cross references with other standards.

9.7 Your Software

The source of a breach can be your company's software, whether it be packaged software from a vendor or custom software developed internally. This book is not a software protection manual, so we won't go into all the potential breaches, but you should know that there are over 30 different potential breaches.

Software security issues can be present not only in custom software, but also in packaged software. Market forces reduce product time-to-market and security is often left as an afterthought, if it's addressed at all. For example, consider how many of the patches for Windows(R) are security patches. Each patch is something that was not thought of at the time the product was created.

9.8 Cyber Security Certifications

There are many possible certifications for cyber security. Listed here are the top five:

- CompTIA Security+
- CEH - Certified Ethical Hacker
- GSEC - GIAC Security Essentials
- CISSP - Certified Information Systems Security Professional
- CISM - Certified Information Security Manager

Each certification certifies a level of knowledge the individual has about cyber security. The certifications differ in difficulty to obtain and in difficulty to keep, so you may want to do some homework about them before hiring someone with a given certificate. The number of offers to hire are greatest by far for CISSP[2].

Generally, certifications are a good thing for your cyber security employees to hold. However, don’t exclude people whose “certifications” come from years and years of experience, but who just haven’t picked up a paper certificate.

9.9 Cyber Security Groups

There are many cyber security groups you can encourage or incentivize key employees to join. Many of these groups maintain websites with lots of cyber security information. I've listed two groups below. The link at the end of this section takes you to a list of 25 groups.

InfraGard

InfraGard is a partnership between the FBI and the private sector. You must join on an individual basis and you must be cleared to Confidential before joining. The clearance process is free, but it takes several weeks. InfraGard provides a wealth of contacts and presentations in the cyber security arena. The group is also a great place to find out about cyber security events and meetings in your area. There is one group near each of the 50+ FBI field offices. Membership is free.

ISSA (Information Systems Security Association)

ISSA is a technical group, although they do sometimes cover the basics. They will help you obtain certifications and alert you to new products and conferences and the like in the area of cyber security. There are approximately 100 chapters in North America, with another 25 or so in South America, Europe, Asia, and Australia. Dues at the time of this writing are about $120 per year plus chapter dues—and most of that goes toward great food at each meeting.

Other Groups

See the link below for 25 more cyber security groups:

http://cybersecurityventures.com/cybersecurity-associations/

9.10 Thinking Outside the Box for Vulnerabilities

Recently, a flaw was found in Internet-connected printers that could allow hackers to attack networks through millions of printers worldwide. It was possible to attack the printer—which led to the network—via email with an infected document sent to the printer. A security researcher demonstrated the ability to rewrite the firmware, keeping the printer penetration undetectable. A quick scan by another researcher in 2011 showed 40,000[8] unprotected printers left open to Internet attack.

By now, this vulnerability has been patched and isn't a worry, but the hackers are busy looking for the next opportunity.

9.11 Insurance

Breaches and identity theft can lead to major expenditures to clean up and recover from. You might want to consider breach insurance and identity theft insurance.

Cyber Liability and Breach Insurance

Cyber liability and breach insurance covers expenses related to a breach and the cost to notify impacted individuals as well as for good faith advertising. Coverage is also available in most states to help cover legal defenses and liability expenses in the event your company is sued. This insurance is generally cheaper than one would think, but the cost is rising as the breaches continue to occur.

Identity Theft Insurance

Identity theft insurance is purchased by individuals. It is often offered free to employees as a benefit or to customers in the case of a breach. Look for the kind that offers to fix the identity theft problem, get the person’s identity back, and cover costs incurred as a result of identity theft.

9.12 Cyber Security Intelligence

Cyber security intelligence is the awareness of what's going on in the world in terms of cyber attacks—what the tools, techniques, and procedures (TTP) of the bad actors are. There are basically three ways to deal with this:

1) Do nothing and hope that your defenses are good enough to cover whatever comes along. Bad idea.

2) Do your own research and analyze each attack and the TTP used along with emerging trends or search daily for public analyses. This is resource expensive, but it has the advantage of scaling for small companies. A partial resource devoted to this is better than nothing.

3) Subscribe to a service that provides this information. Let them do the research and use their trained and experienced staff for the analysis. Examples of these services are FireEye, Forcepoint, and Verisign. For a list of others, search for "threat intelligence companies."

Another option not numbered with the above, as it can be employed in addition, is to join one of the industry ISAC's (Information Sharing and Analysis Center) that shares threat information. Follow this link to join: http://www.nationalisacs.org/#!member-isacs/jnog6

From awareness, training, and culture to certifications and sharing ideas, there is much your company can do to reduce your cyber security risk. We'll next look at reducing your company's potential liability in the event of an "incident" or breach.

10.0 Reducing the Liability at Your Company

A little preparation goes a long way toward preventing a breach and reducing potential liability for your company when a breach occurs.

10.1 Policies and Procedures

If you are not already familiar with “policies and procedures,” it is a set of principles, rules, and guidelines describing what should be done for each policy area in your company. An example of a policy is that computer and network backups should be performed with a specific frequency as a good protection against ransomware. A procedure would detail by whom and how the backup(s) should be performed.

A policies and procedures manual or book is typically printed, so that it is accessible by all employees. Many times the manual is available through a company’s intranet, which makes updates to the manual easy to manage.

If you haven’t already put cyber security policies in place, check out this site—it has 25 security policies to get you started:
http://www.comptechdoc.org/independent/security/policies/

A word of caution, though. Don’t just adopt someone else’s policies. Think them through and adjust them for your company. Make them your own. Also, check with your HR department—they have a lot of experience in writing policies. See also **Section 9.6 NIST Cyber Security Framework** for some suggested cyber security policies and procedures.

Having written policies and procedures will reduce your liability in the case of a breach. The effectiveness of the policies and procedures depends on each employee not only being aware of them, but also understanding and following them.

10.2 Best Practices / Due Diligence

Implementation of cyber security “best practices” for your type of business and size of company constitutes “due diligence” which protects against triple damages in any class action awards. Unfortunately, there is no agreement on what constitutes “best practices.” Following the NIST Cyber Security Framework document, discussed above in **Section 9.6 NIST Cyber Security Framework**, would be a good start.

If your company is large enough to have a board of directors, get them involved in cyber security and provide training for them.

Finally, listen to the cyber security professionals at your organization when crafting your policies and plans. According to a recent survey, 66% of IT professionals think their company’s cyber incident response plans are not up to the task.[23] This indicates to me two things: that the cost of appropriate defenses is always too high and that not enough listening to the guys and gals in the trenches is occurring.

10.3 Preparing for a Breach

In terms of potential breaches, the advantage is all with the attacker, because the bad actor only needs to find a single entry point that is not guarded, while you have to guard thousands of entry points in your systems. Not fair, but that's the current reality.

No matter what you do to prepare, the actual breach will not be what you expected—it's like "the fog of war"—but *any preparation* is much better than *no preparation*. Have a plan. Be prepared to make some adjustments to it. See **Section 10.6 Learning from the Breach** below.

In your preparations, include a plan for the period of time between when the breach is discovered and when the breach is sealed and all vestiges of the malware are out of your system. For a period of time after the Sony attack, Sony disconnected from the Internet and relied on inter-office memos and fax machines to communicate.[28]

Defensive Tactics and Solutions

- Use table top exercises[27] to practice a simulated breach to see if everyone knows what to do and if what they are supposed to do makes sense. The FBI can advise you on running a table top exercise. Remember, a table top exercise is about improvements, not about finding people to criticize.
- Review your plans at least annually. Address any new threats that have surfaced. For example, ransomware wasn't a big deal a few years back.

10.4 Help from the US Government

The FBI offers help in developing press releases before and after the breach and in finding out who did it. It also provides general tips for improving your cyber security. It is best to form a relationship with your local FBI office *before* the need arises and then to keep their phone number handy.[4] Help from the FBI before and after will also be a plus when it comes to "due diligence," discussed in **Section 10.2 Best Practices / Due Diligence** above.

The Department of Homeland Security (DHS) also offers help with cyber incidents through their US-CERT (United States Computer Emergency Readiness Team), ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), and NCCIC (National Cybersecurity & Communications Integration Center) organizations.[26]

10.5 After the Breach and Breach Mitigation

A good percentage of businesses are out of business within five years of a breach, so it is important that you take this seriously both before and after.

The first thing to do is to call it an "incident" until it becomes clear that a breach *has* occurred. Once the term "breach" is used, a clock starts on how long your firm has to make notifications under several applicable laws. HIPAA includes a notification in its law and there's a new one from the FTC. Check with a knowledgeable cyber security lawyer to determine your obligations. The penalties for non-timely reporting are stiff and can be a *per record* fine in the case of HIPAA.

You will also need to notify all stakeholders such as your board of directors, employees, customers, suppliers, and the public. Fast, accurate action is necessary to preserve good will. You will also need some extra cyber security actions to assuage future fears and to be prepared to answer the question, "Why didn't you take these steps earlier?"

Discovering a breach and sealing it does *not* mean your systems are safe. A good hacker will leave behind an APT (Advanced Persistent Threat) which is difficult to find and remove from your systems. The bad actor only has to leave one behind—but could leave thousands. Consider the time and effort it could take to find and remove those. Proving your system is once again safe from a breach is not always easy to do.

Summary of Breach Mitigation Steps for Your Organization

- Stop the immediate breach.
- Determine the impact.
- Notify those impacted.
- Comply with regulatory reporting requirements.
- Insure breach is really sealed.

Steps are not necessarily in order and may occur simultaneously.

If you want more help in this area, consider the NIST Special Publication 800-184 entitled "Guide for Cybersecurity Event Recovery" which is still in draft status[29] at this writing:

http://csrc.nist.gov/publications/drafts/800-184/sp800_184_draft.pdf

10.6 Learning from the Breach

Think process improvement. How did they get in? What can we do to stop that? How did our “after breach” processes work? Do we need to modify them? How comfortable are we with our existing cyber security? Is it time for an outside audit? Do we need to review the cyber security budget? Where are we scoring as a company on the NIST Cyber Security Framework? (See **Section 9.6 NIST Cyber Security Framework**.) Do our employees and contractors need more cyber security training?

Being breached is bad enough, but being breached again using the very same technique two months later is tragic. Learn from your mistakes and weaknesses.

There are many types of products available to help with your cyber security. We’ll look at some of them in the next chapter.

11.0 A Look at Some Cyber Security Products

Various types of products to help with your cyber security are available and some are described below. This is not intended to a be a comprehensive list or an endorsed list, but rather an example of products in the various categories. Note that in those products provided by Secure Web Apps, there is an inherent author bias. Open source applications are designated with OS, free with F, and proprietary with P.

11.1 Virus Checking

Virus checking programs can run continuously or at intervals to check for viruses among the files on the data storage of the device. They also must, at intervals, download new malware signatures to aid in detection of the new viruses created daily.

Norton(R) **AntiVirus** (P) by Norton – defends against viruses, spyware, malware, and other online threats.

Norton(R) **360** (P) by Norton – antivirus, online protection, and PC performance tuning. Currently being replaced by Norton Security Premium.

McAfee(R) **Virus Checking** (P) by McAfee – virus protection by another well-known vendor.

ClamAVTM **(Clam AntiVirus)** (OS) – roughly equivalent to Norton AntiVirus, except the price is lower. ClamAV can be used in conjunction with Malwarebytes for more complete protection.

MalwarebytesTM **Anti-Malware** (F, P) – roughly equivalent to Norton 360. You can download the free version and see what you think before you purchase it.

11.2 End Point Security

End point security is comprised of solutions that provide security for mobile devices or various types of workstations, such as desktops and laptops.

For Linux:

DrawBridge 1000™ (P) by Secure Web Apps – provides phishing protection, malware protection, and hardening for Ubuntu™ and Debian(R) workstations.

For mobile devices:

MaaS360(R) (P) by IBM – provides a solution to secure your mobile devices, apps, and content along with a mobile device management solution.

For Windows:

Endpoint Security Remediation Suite™ (P) by Thycotic – provides privilege management and security, application controls, and group management for Windows endpoints.

11.3 Server Security

Servers are the larger computers that are used for websites and web applications either at on organization or at an ISP. Servers are also used for printing, storing files and documents, and more.

For Linux:

Fortress 1000™ and Sentinel 1000™ (P) by Secure Web Apps – provide multiple level cyber security defenses and monitoring for Ubuntu™ and Debian™ servers. Protections include stealth, malware protection, DDos scrubbing, intrusion prevention, intrusion detection, attack surface reduction, email alerts, antivirus, firewall enhancement, permissions audit, bad IP protection, availability checking, and updates during license period to keep up with current threats.

For Windows:

F-Secure Server Security Premium™ (P) by F-Secure – a JAVA based application that provides spam filtering, remote collection of diagnostics reports, botnet blocker, and web traffic scanning and protection.

11.4 Application Security

An application is a program or programs that function together to provide a service to the user. An example of this is a word processor. An application could be made specifically to run on a desktop or a phone or could be a web application that is accessible from all your devices and actually resides upon a server.

PHP LAMP Stack:

Barrier 3000™ (P) by Secure Web Apps – Rapid web application development framework with security included for PHP/MySQL. Speeds up application development and is skinnable to match client branding. Defends against these attacks: semantic URL, file upload, CSS, cross site request forgeries, spoofed HTTP requests, exposed access credentials, SQL injection, exposed session data, backdoor URL's, filename manipulation, code injection, traversing the file system, remote file attacks, command injection, brute force attacks, password sniffing, replay attacks. Features: user groups, unique menu per group, access controls, reporting, graphics, data editing, logging, data models, mapping, mobile support, Ajax cascade, active directory login or web login.

Multiple Platforms and Languages:

Arxan™ (P) by Arxan Technologies – provides protection for various types of applications running on a variety of platforms. It defends against attacks, detects when an attack is being attempted, and responds with alerts and repairs.

11.5 Network Security

Advanced Malware Protection(R) by Cisco (P) – a hardware device for enterprises that protects against highly sophisticated and targeted malware.

Advanced Malware Protection is a registered trademark of Cisco.

11.6 Code Scanners

Code scanners are programs used by programmers or testers to scan programs looking for real or potential security holes.

Vega™ (OS) by Subgraph – a vulnerability scanner that supports security testing of a web application. Written in Java, it works for OSX, Linux, and Windows.

Fortify on Demand(R) (P) by Hewlett Packard – several solutions for scanning software code and for managed security testing.

11.7 Application Security Testing Tools

Application security testing tools are used to test application software for security holes.

w3af (OS) – an attack and audit application for web application penetration testing. This tool claims to be able to identify over 200 kinds of web application vulnerabilities.

sqlmap (OS) – tests web applications for SQL injection vulnerabilities.

11.8 Ad Blockers / Anonymity Tools

Ad blockers keep your web browser from downloading ads. Anonymity tools block any tracking of the sites you visit by anyone except the search engine used to find them.

Adblock Plus™ (F) by Eyeo GmbH (German company) – blocks all ads from your webpage. Some sites are starting to detect this and will block you from entering their sites. You can choose to not enter the site or to allow just that site's ads to appear.

Ghostery® (F) by Ghostery – blocks all cookie trackers, so no one knows where you visit on the web.

Do your research, talk to your IT teams, and determine your best route to cyber security!

12.0 Final Thoughts …

We have covered many different cyber security topics in a short time and have covered each in an introductory manner. More detailed and technical information on each topic is available from other sources.

The bad actors are constantly working against us—always coming up with something new. I had to go back and add to this book more than once, because a new type of attack became available during the course of writing. Some types of attack are newer yet. For example, I have recently heard the term “whaling” bandied about, which is phishing for the really big fish. In whaling, a whole team of people is assigned to just one person.

I hope this book has helped you to consider the issues and to better prepare your family and business against cyber risk. I hope that you will share this book with friends and neighbors, so they, too, are cyber secure.

If You Live in a Country other than the United States

This book is admittedly a bit US-centric with references to the FBI, DHS, HIPAA, and so on; however, I hope you will ignore those US-centric items and consider the advice contained herein because cyber security is a universal need.

Most country governments offer some type of cyber security advice or service. A few are listed here in no particular order:

Italy:

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf

United Kingdom:

http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

India:

http://deity.gov.in/content/cyber-laws-security

European Union:

https://www.enisa.europa.eu/

Indonesia:

http://www.opengovasia.com/articles/6563-indonesia-launches-cyber-security-agency-in-wake-of-growing-threat-landscape

Australia:

http://www.asd.gov.au/infosec/acsc.htm

Japan:

http://www.nisc.go.jp/eng/

Canada:

https://www.cse-cst.gc.ca/en/group-groupe/cyber-defence

Glossary of Cyber Security Terms

This glossary contains special terms applied to cyber security. Many of these words have a different meaning in another context. This is not a complete glossary, since some of the cyber security terms about the details of networking don't apply to this book. At the same time, some of the terms below aren't found in this book, but should help you better understand news reports about cyber security events.

Access – the ability to utilize a portion of a device and ask it to perform actions—related most often to data—on your behalf.

Access Control / Access Control List (ACL) – a list of what the user of a device can access or use on that device.

Actor State – a nation involved in hacking activities.

Adware – software that displays unwanted ads.

Air Gap – a security measure in which a system is isolated, that is, it can't be reached via the Internet, the corporate network, or otherwise. A system can be described as "air gapped" from the rest of the network.

Application – a program or programs that function together to provide a service to the user.

APT / Advanced Persistent Threat – a bad actor with sophisticated levels of expertise and large resources which allow it to achieve objectives using multiple attack vectors.

Attacker – another name for hacker, a group of hackers, or even an actor state.

Attack Surface – the amount of exposure to attack in a system, such as a computer, a network, or a network plus one or more computers.

Backdoor – a means of access to a device that bypasses the normal security mechanisms.

Bad Actor – not a person with poor acting skills—rather, someone who is attempting to perpetrate "bad" upon your cyber systems.

Biometrics – the technology of authenticating identity based on fingerprints, iris scans, or other body uniqueness. Biometrics can be used in place of or in addition to passwords.

Bitcoin – a method of payment on the Dark Web.

Black Hat Hacker – a hacker who finds and then exploits computer system weaknesses and does not notify anyone. The information is kept for use by the hacker or the hacker's organization.

Blue Team – a group of cyber security experts who are defending a system. Blue teams are often played against red teams in an effort to tighten security.

Bot – a compromised computer attached to the Internet that uses remote control to perform activities directed at other computers on the Internet.

Botnet – a network of bots often used for DDos attacks.

Breach – the penetration of a device or network by a bad actor resulting in access to data contained therein, a compromise of the function of said device, or a kinetic side effect.

Container – a way to package up an application and all its dependencies. Generally not as secure as using virtual servers.

Cryptography – the use of mathematical techniques to provide confidentiality, data integrity, entity authentication, and data origin authentication.

Cyber – a word derived from cybernetics that refers to anything related to computers.

Cyber Security – software, configuration, actions, policies, training, and preparation taken to secure one's cyberspace.

Cyberspace – various networks used in information technology infrastructure that include devices, the Internet, and data. Cyberspace can also be defined as an electronic medium in which communications take place on the Internet.

Cyber Warfare – actions taken by actor states to breach the defenses (cyber security) of the cyberspace of their opposition. Russia has used this recently in conjunction with regular warfare and hence the term "hybrid warfare." Another name for this, in some instances, is "cyber terrorism."

Dark Web – sites on the Internet that hide their identity and IP addresses using encryption. These sites are not accessible from the standard search engines and are used by hackers and others for nefarious purposes.

Data Diddling – altering some of the contents of data to make the data untrustworthy.

DDos Attack / Distributed Denial of Service Attack – an attack done by sending valid requests to the server in such numbers that the responses overwhelm the server; the server then does not have enough horsepower (CPU cycles) to respond to legitimate requests. This renders the server as though it were offline or ineffective.

Decryption – the opposite of encryption; the use of the encryption key and the encrypted data to extract the original, unencrypted data.

Defense in Depth – multiple layers of defense to make penetration of a system very difficult.

DMZ / Demilitarized Zone – think of this as a network and components that are between a trusted network and one that is untrusted, thus protecting the trusted network.

DNS (Domain Name System) Server – a server that translates from a domain name—such as 'mysite.com'—to the IP address of the server the site is on—such as 192.112.34.34.

Encryption – the conversion of data into a form that is not decipherable. The quality of the encryption determines whether or not it can be decrypted by the wrong person.

Exfiltration – a military term applied to data, meaning the data's removal from the system by an attacker. It is one thing to attack a system and get in—and another to get the data off the system.

External PEN Test – penetration testing done from outside the system and without a login. This attempts to mimic an attacker to see if the system is easy to breach.

Firewall – a group of components (hardware and/or software) that forms a barrier between two networks or between a network and a device.

Hacker – one who attempts to circumvent a computer's or a network's security. A hacker can be good or bad (see also **Black Hat Hacker** and **White Hat Hacker**).
Honeypot – a server containing nothing of value that is installed to measure the types of attacks being used.

Incident – a term used to indicate "something has happened, but we aren't sure what it is." The term is used until it's determined that a breach has occurred.

Incident Response Plan – a written plan of what an organization needs to do in the case of an incident or a breach.

Information Assurance – the practice of managing risks related to information.

Insider Threat – the theft of information, sabotage, or theft of credentials by someone who has legitimate access to the client's system.

Internal PEN Test – penetration testing from inside using a valid login to see what hacking can be done using the login.

Intrusion Detection – the act of detecting when a computer, server, or network has been entered by software that doesn't belong there.

IoT / Internet of Things – the attachment of physical objects, devices, vehicles, and buildings to the Internet either though a hard-wired connection or through Wi-Fi.

IP Address – the address of your device on the Internet. The old address standard was IPv4 (32-bit scheme) which was upgraded to IPv6 (128-bit scheme) to prepare for the expected avalanche of addresses needed for IoT devices.

ISP / Internet Service Provider – a company that provides access to the Internet. Some examples are Time Warner Cable, AT&T, Google, and Verizon.

Keylogger – software that logs all your keystrokes to a file and then exfiltrates that file to another computer. A good way to steal logins and passwords.

Layered Defense – see **Defense in Depth**.

Login or Log In – the action of identifying yourself to the system in a manner that it knows who you are. With a valid login, the system allows you to take actions upon it based on its Access Control List (ACL) settings for you.

Malware – software that compromises the operation of a device or network by performing an unauthorized function.

Malware Signature – a group of bytes of code (a portion of the malware program) that is unique to that malware, thus becoming its "signature."

NIST – National Institute of Standards and Technology and keeper of the cyber security standards for FISMA, the government information security standard.

NIST Cyber Security Framework – published in 2014, this framework is short in length (less than 40 pages) and is an attempt to guide an organization from where it is in cyber security to the next level.

Password – a unique combination of letters, numbers, and special characters known only to you and the computer you are attempting to gain access to.

PEN Testing – penetration testing or simulated attacks on the system to gain entry.

Penetration – gaining entry to a system.

Phishing – the sending of emails to many people, hoping to snag someone who will open the email and then click on a link or run an attachment. The link or attachment is designed to compromise the receiver's system.

Polymorphic Malware – malware that can modify its own signature while running.

Ransomware – software that encrypts a computer or a database and then demands a ransom be paid, often in bitcoins. When the ransom is paid, the decryption key is given to the victim who can then recover the encrypted data.

Red Team – a group of cyber security specialists who attack just like the bad actors in order to test defenses.

Revenge Porn – the release of photos or text shared digitally to the general public as a means of revenge. (See **Sexting**)

Risk – the potential for an unwanted outcome to occur.

Risk Management – management of risk through controlling it to an acceptable level. There is always a tradeoff between risk and cost of the risk mitigation efforts.

Root Kit – software tool with administrator privileges installed on a device and designed to maintain its presence and avoid detection while still being able to function.

Security Hole – something not right that could allow a hacker to penetrate the system, be it an application, a server, a workstation, or a network.

Sexting – sharing of sexually provocative photos or text with another using digital means.

Spear Phishing – a highly targeted phishing campaign directed against a population as small as one person. Much more research and effort goes into making this email (as opposed to a phishing email) seem real to the reader. (See **Phishing**)

Spoofing – a situation in which a person or a program masquerades as another by falsifying data. The masquerade enables the spoofer to gain the person's permissions or causes the attribution of the spoofer's actions to the other person or program.

Spyware – software that enables spying upon the activities of a user or a computer by transmitting information from a computer without being detected.

SSL / TLS – protocols providing data encryption and authentication between a computer (server) and a user's browser. SSL (Secure Sockets Layer) has proven vulnerable and is being replaced by TLS (Transport Layer Security).

System – a computer, a network, or a network and one or more computers.

Threat – a circumstance or event that claims to or has the potential to exploit vulnerabilities and to adversely impact an organization.

Threat Vector – the way the threat attempts to enter a system. For example, the threat vector for a phishing campaign is initially an email that contains a link or an attachment. The malware is deposited on the system by opening the link or executing the attachment.

Trojan – another name for Trojan Horse. It's benign in appearance—as in having a useful function—but hidden within is a potentially malicious function.

TTP / tactics, techniques and procedures (sometimes tools, techniques, and procedures) **–** the signature method of the bad actor. Work can often be attributed to a bad actor by looking for the TTP. Think *modus operandi*, in law enforcement terms.

Two Factor Authentication – the use of more than one medium to log in. For example, the regular login may trigger the sending of a PIN to the user's email or phone that must also be entered to complete the login.

VPN / Virtual Private Network – a temporary encrypted link over the Internet between two points which creates a private network of shared resources that are not accessible to the outside world.

Virus – a computer program that can infect a computer and then replicate itself and spread —usually through attachment to a document, program, or email—to other computers in a network.

Virus Checker – a program installed on a workstation or server that protects against viruses by looking for a virus's signature and then quarantining the file so it cannot run on the computer.

Vulnerability – a portion of a system that is weak and can be attacked. For example, a piece of software with a bug in it that allows attack, a system whose patches have not been applied, and so on.

White Hat Hacker – one of the good guys who hacks systems to find vulnerabilities. The white hat hacker lets the owner know, so the vulnerability can be fixed.

Worm – a self-replicating, self-propagating program that uses a network to spread itself.

Zero Day Virus – a virus with a signature not yet recognized by virus checkers. Often used with spear phishing to gain access.

References

[1] Scannell, Kara (2016, February 24) *CEO* Email Scam Costs Companies $2bn *Technology*. Retrieved from http://www.ft.com/cms/s/0/83b4e9be-db16-11e5-a72f-1e7744c66818.html

[2] Tittel, Ed (2015, September 3) Best Information Security Certifications for 2016 *Tom's IT Pro*. Retrieved from http://www.tomsitpro.com/articles/information-security-certifications,2-205.html

[3] (2014, March 20) *Phys.Org* WPS2 wireless Security Cracked Retrieved from http://phys.org/news/2014-03-wpa2-wireless.html

[4] (no date) *The Federal Bureau of Investigation* Computer Intrusions Retrieved from https://www.fbi.gov/about-us/investigate/cyber/computer-intrusions

[5] Humer, Caroline and Finkle, Jim (2014, September 24) *Reuters* Your Medical Record is Worth More to Hackers Than Your Credit Card Retrieved from http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[6] (2016, March 1) *Reuters* NSA Chief Says 'When, Not If' Foreign Country Hacks U.S. Infrastructure Retrieved from http://fortune.com/2016/03/01/nsa-chief-hacking-infrastructure/

[7] MacDonald, Elizabeth (2016, February 2) *FOXBusiness* Washington Moves to Thwart U.S. Power Grid Attacks Retrieved from http://www.foxbusiness.com/features/2016/02/02/washington-moves-to-thwart-u-s-power-grid-attacks.html

[8] (2011, November 29) *NBCNews* Exclusive: Millions of printers open to devastating hack attack, researchers say. Retrieved from http://www.nbcnews.com/business/consumer/exclusive-millions-printers-open-devastating-hack-attack-researchers-say-f118851

[9] Brandom, Russell (2016, May 2) *The Verge* Your Phone's biggest vulnerability is your fingerprint Retrieved from http://www.theverge.com/2016/5/2/11540962/iphone-samsung-

fingerprint-duplicate-hack-security

[10] Korolov, Maria (2015, April 10) *CSO* Surveys: Employees at Fault in the Majority of Breeches Retrieved from http://www.csoonline.com/article/2908475/security-awareness/surveys-employees-at-fault-in-majority-of-breaches.html

[11] OPM Cybersecurity Resource Center Cybersecurity Incidents Retrieved from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[12] Boyd, Aaron (2015, June 25) *Federal Times* Contractor breach gave hackers keys to OPM data Retrieved from http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277/

[13] Wallace, Gregory (2013, December 23) *CNN Money* Target credit card hack: What you need to know" Retrieved from http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/

[14] Bayly, Lucy (2016, April 6) *NBC News* Cybercriminal raise rates, work harder for all your hacking needs Retrieved from http://www.nbcnews.com/tech/tech-news/cybercriminals-raise-rates-work-harder-all-your-hacking-needs-n551886

[15] (2015, October 8) Top 10 countries with most hackers-cyber criminals Retrieved from: http://www.countrydetail.com/top-10-countries-with-most-hackers-cyber-criminals/

[16] Gertz, Andrew (2016, March 3) *Enterprise Security* 2015 Data breach Statistics: The Good, the Bad and the Ugly Retrieved from: http://blog.gemalto.com/security/2016/03/03/2015-data-breaches-by-the-numbers/

[17] Fox-Brewster, Thomas (2015, December 28) *Forbes* 191 Million US Voter Registration Records Leaked in Mysterious Database Retrieved from: http://www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/#3bb4eb311bb9

[18] Noyes, Katherine (2016, June 15) *CSO* Cost of a data breach: $4 million. Benefits of responding quickly: Priceless. Retrieved from: http://www.csoonline.com/article/3083931/security/cost-of-a-data-breach-4-million-benefits-of-responding-quickly-priceless.html

[19] Kan, Michael (2016, June 30) *IDG News Service (PCWorld)* Mobile ransomware use jumps, blocking access to phones. Retrieved from: http://www.pcworld.com/article/3090049/security/mobile-ransomware-use-jumps-blocking-access-to-phones.html

[20] Aftab, Perry (2016, March) *Wired Safety* What is Cyberstalking and Cyberharassment? Retrieved from: http://www.wiredsafety.com/#!parry-aftabs-did-u-know–cyberstalking/c200f

[21] Aftab, Perry (2016, March) *Wired Safety* Sexting, Sextortion and Revenge Porn Retrieved from: http://www.wiredsafety.com/#!sexting-sextortion-and-revenge-porn/cptj

[22] Korolov, Maria (2016, June 20) *CSO* Spearfishing attacks target boards Retrieved from: http://www.csoonline.com/article/3085492/security/spearphishing-attacks-target-boards.html

[23] Barth, Bradley (2016, June 13) *SC Magazine* Survey: 66% of IT pros think their companies' cyber incident response plans are ineffective Retrieved from: http://www.scmagazine.com/survey-66-of-it-pros-think-their-companies-cyberincident-response-plans-are-ineffective/article/502798

[24] (2016, June 16) *Security Week* Losses From Business Email Compromise Scams Top $3.1 Billion Retrieved from: http://www.securityweek.com/losses-business-email-compromise-scams-top-31-billion-fbi

[25] Timm, Trevor (2016, June 29) *Columbia Journalism Review* What media companies don't want you to know about ad blockers Retrieved from: http://www.cjr.org/opinion/ad_blockers_malware_new_york_times.php

[26] *Homeland Security* Cyber Incident Response Retrieved from: https://www.dhs.gov/cyber-incident-response

[27] Malec, Joe (2015, Sept 21) *Info Security* Incident Response Tabletop Exercises for Beginners Retrieved from: http://www.infosecurity-magazine.com/opinions/inc-resp-beginners/

[28] *Inform Micro Advisor (Cisco)* An In-depth Look at the Timeline of a Security Breach Retrieved from: http://www.ingrammicroadvisor.com/cisco/blog/an-in-depth-look-at-the-

timeline-of-a-security-breach

[29] *NIST* Draft NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery Retrieved from: http://csrc.nist.gov/publications/drafts/800-184/sp800_184_draft.pdf

[30] Greenburg, Andy (2015, July 21) *Wired* Hackers Remotely Kill a Jeep on the Highway - With Me In It Retrieved from: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[31] Tung, Liam (2016, July 18) *ZDNet* This webcam malware could blackmail you into leaking company secrets Retrieved from: http://www.zdnet.com/article/this-webcam-malware-could-blackmail-you-into-leaking-company-secrets/

[32] Iyer, Kavita (2016, July 27) *TechWorm* BlackBerry announces DTEK50 Android smartphone, "the world's most secure phone." Retrieved from: http://www.techworm.net/2016/07/blackberry-announces-dtek50-android-smartphone-worlds-secure-phone.html

[33] Seals, Tary (2016) *InfoSecurity* Visual Hacking is Successful 91% of the Time Retrieved from: http://www.infosecurity-magazine.com/news/visual-hacking-is-successful-91-of/

About The Author

The author, Walter L. Turner, is Vice President at Secure Web Apps, a cyber security and web software company. He has been fascinated with IT since he built his first computer after finishing two master's degrees by the age of 21. Adept in 13 programming languages, Walt has done system, application, real time embedded, operating system, simulation, and web programming in his long and illustrious career. He has also served as a server administrator, data base designer, test team leader, manager, director, and president. Walt has consulted in over 17 industries.

Walt was first exposed to cyber security in the 1980's when tasked with a project to provide networking to 280+ correspondent banks. His contributions, innovative for the time, were honeypots, time of day and week controls, extra authentication, protocols, and the use of red (attack) and blue (defense) teams to improve the cyber security design.

He followed this by integrating cyber security testing into the test team for a world-wide logistics system for a subdivision of American Airlines.

Walt then took 14 years out to teach computer science including becoming department chair. While chair, he grew the department by 500%. His graduates were sought out by industry and held the all-time, all-major starting salary record for many years.

Walt began work on web applications in 1995, the year after the Internet became available. His first project? A 1,500-page website done using students. This is where he says he got his gray hair. Next up was a 100-page portal that was never hacked in spite of existing outside the firewall.

A 450-page, 7-volume cyber security design for a programming framework to meet FISMA, HIPAA, and PCI requirements was next for Walt, while working at Corporate Web Consulting.

Walt is currently the Vice President at Secure Web Apps which offers cyber security products for server, workstation, and web application protection. More details can be found on their website at https://SecureWebapps.com.

Walt is a native of Kansas, but has lived in the South for the last many years. He claims to have a working knowledge of Southern. His hobbies are woodworking, remodeling, reading, movie watching, and kid raisin'. Walt and his wife have nine children.

Walt would love to hear your comments. Write him at: cybersec4u@SecureWebApps.com.