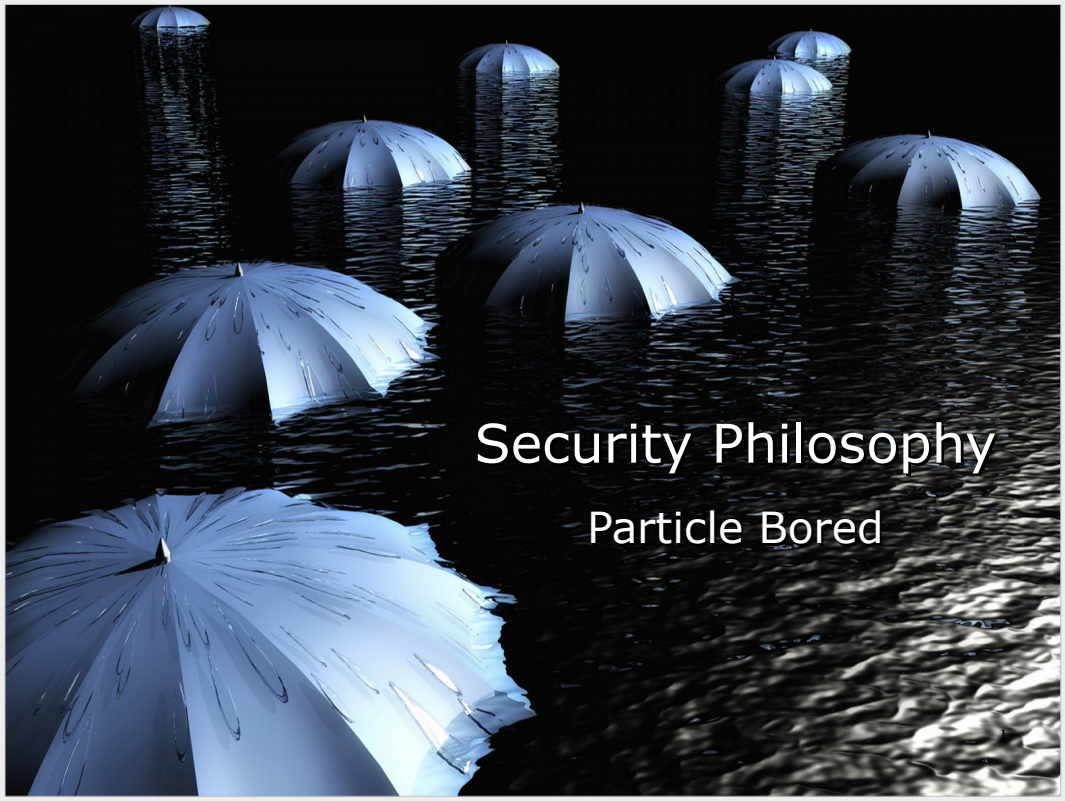

Security Philosophy
Particle Bored

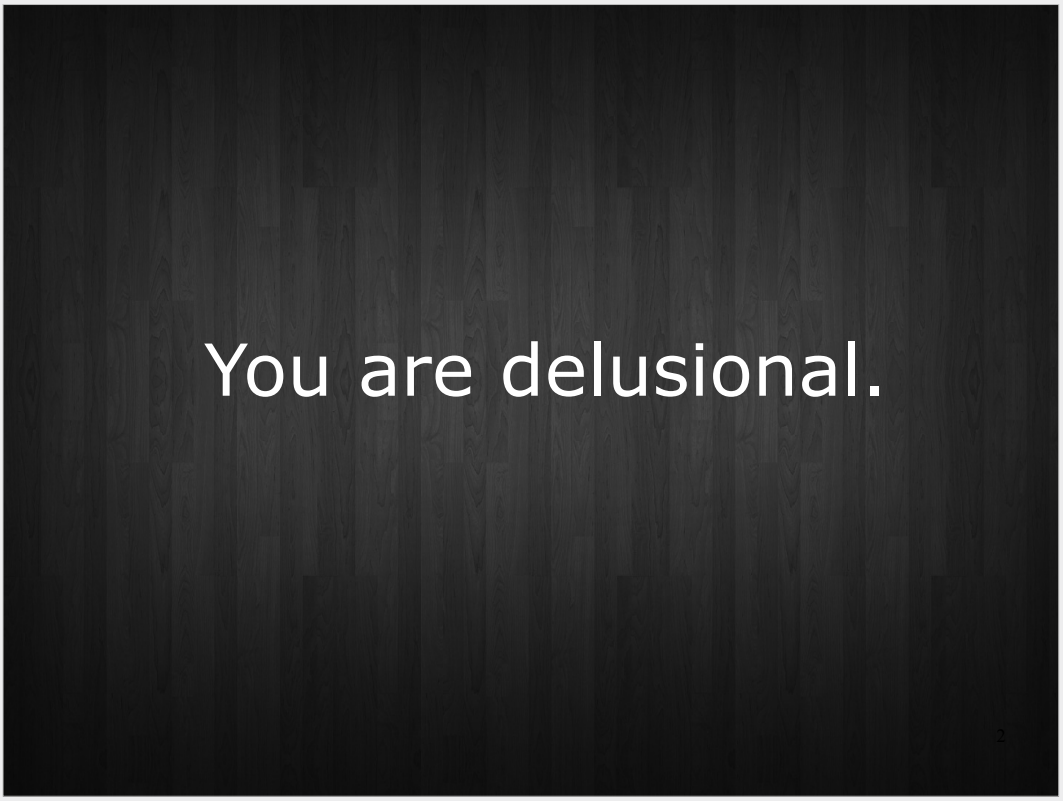


This image is a pretty good analogy for the security posture of most of us – if you can imagine people holding up the umbrellas. Our security controls may do a great job of preventing rain from falling directly on our heads but we are still drowning.

So today I would like to share some concepts I have learned that will help you begin to fix this problem.

Let's start with the biggest concept of all:

Would you like to know the primary cause of absolutely all of your security issues?



Please don't take this as a personal attack – this is pretty exciting stuff so I need you to pay attention.

I don't have time to go into all of the reasons why you are delusional but the important thing to remember is your perception of reality is not quite right. And it is this small difference between the way you think the world works and the way it really works that creates an opportunity for your attacker.

The great thing is that if most security problems are caused by your misunderstanding of reality then that is something you are completely empowered to fix. You will never be able to defend against the “unknown unknowns” but you should be able to take care of everything else.

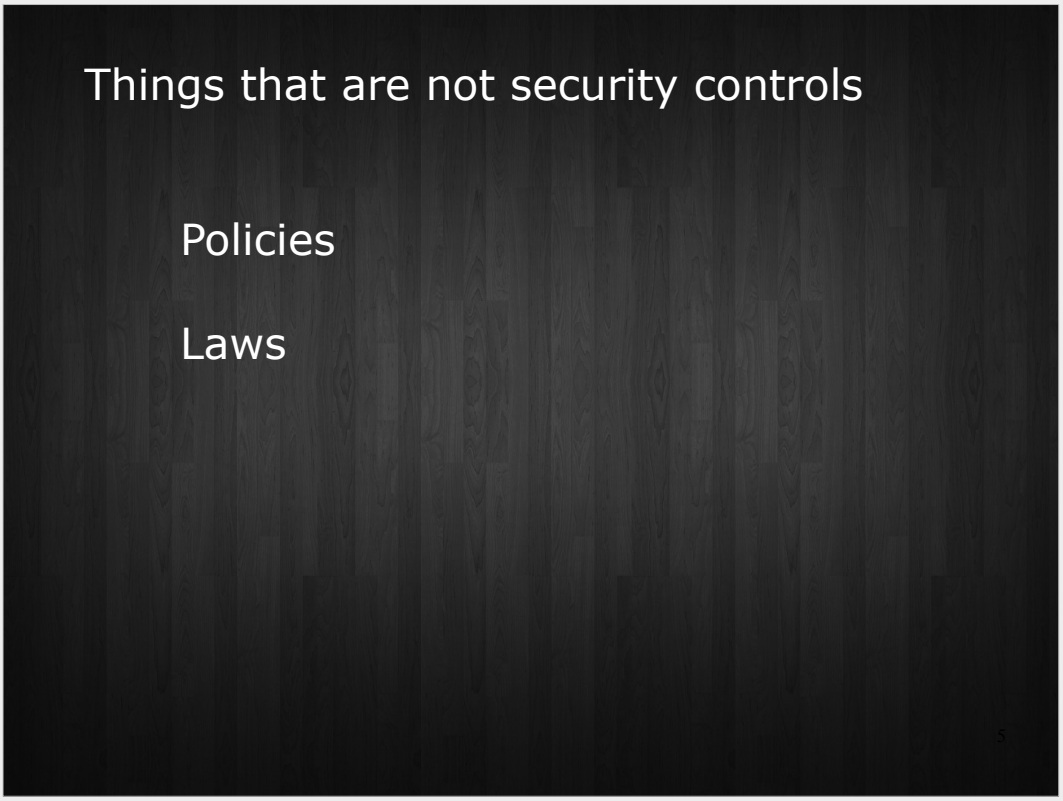
So the remainder of this talk will help you dispel your delusions.

There are a few things that people rely on as security controls but they really are not.

Policies are just words on a piece of paper so they can't physically stop bad things from happening.

But if you look around your organization you may find cases where policies are the only thing you have been able to get done so you still don't have any real controls.

For example, you may have a policy that prohibits flash drives but did you ever get approval to buy the software you need to physically prevent people from using them? Maybe not.



Laws are just another written policy. If all you have done is write a law then you have not done anything to stop an attacker yet.

Hiding something does not prevent it from being stolen.

At some point your secret will be accidentally revealed, actively discovered, or intentionally given away by someone you trust.

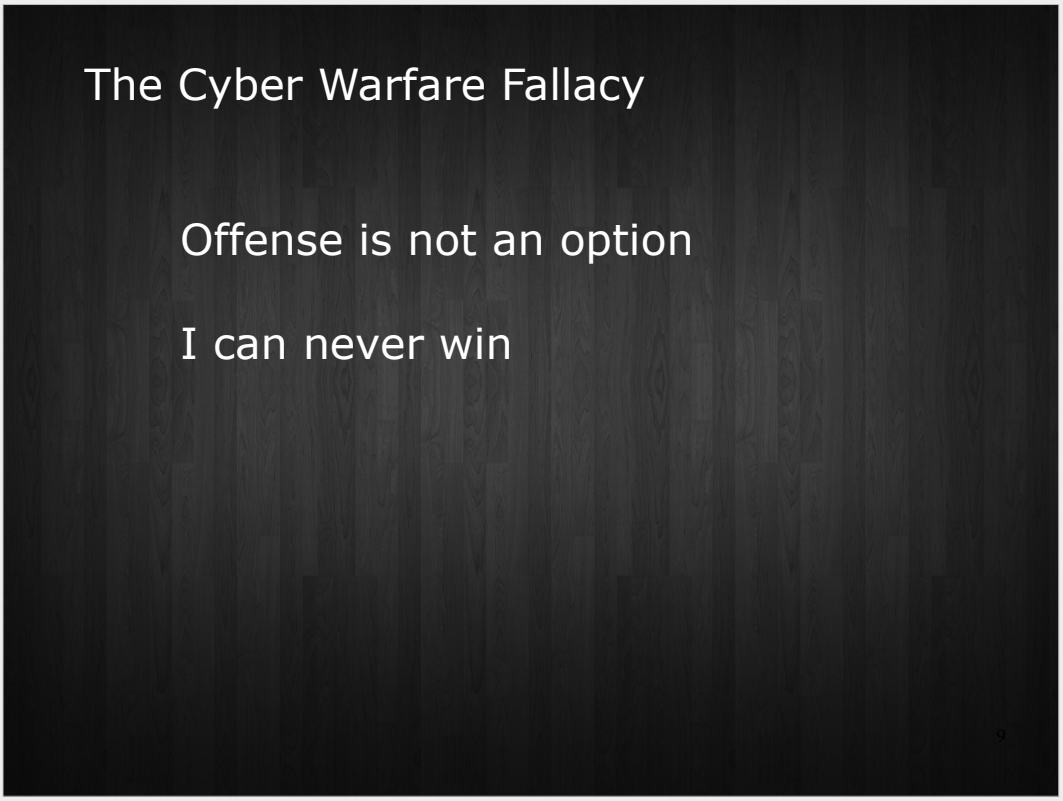
There are currently nearly one million people who have a United States Top Secret security clearance. There is absolutely no chance that every single one of them will keep their mouths shut about everything, forever.

Laws and obfuscation also help explain why things like software vulnerabilities happen. Vendors don't want to pay to secure their stuff so they try to hide their flaws by saying you are not allowed to reverse engineer their products. But user agreements don't physically stop people from reverse engineering things so people eventually find the problems the vendor didn't look for.

There has been a lot of hype about cyberwar lately but there are a few reasons why I am not “buying” it.

Most of us have no offensive capability.

I may be able to determine that someone is about to attack my web site but that does not give me the right to attack them first. In fact I'm not allowed to attack them even after they start attacking me.



If I thwart your attack on my web server that is not a victory.

Since I can not attack you I have no way to decrease your resources or capabilities.

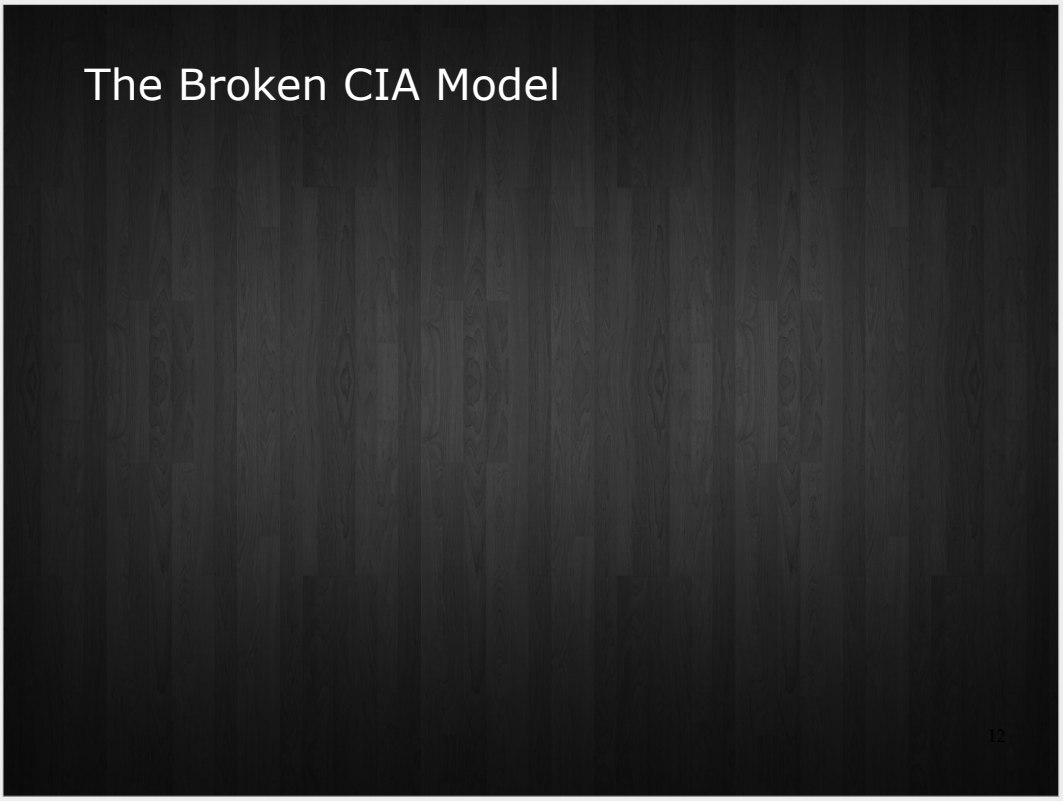
You ultimately become even stronger after attacking me due to what you learn about my response.

Cyberspace is a completely arbitrary and synthetic environment. If you were to take away electricity the entire thing would completely disappear. One of the consequences of this is that absolutely everything on the Internet can theoretically be counterfeited.

So if you can't trust anything you see on the Internet, how can you effectively respond to things that appear to be a problem?

We all share the same infrastructure so I can't attack you without hurting myself.

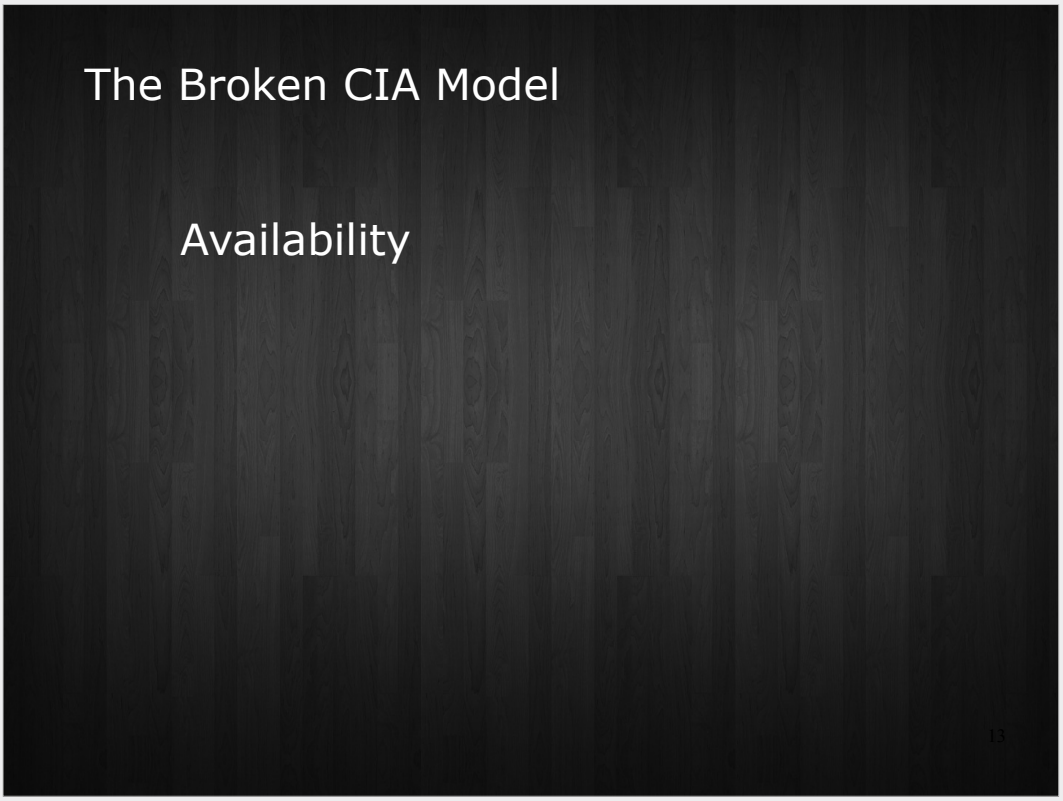
For example, I am pretty certain the United States could take out China's power grid if they wanted to, but that would slow the production of iPads which most of us could not tolerate.



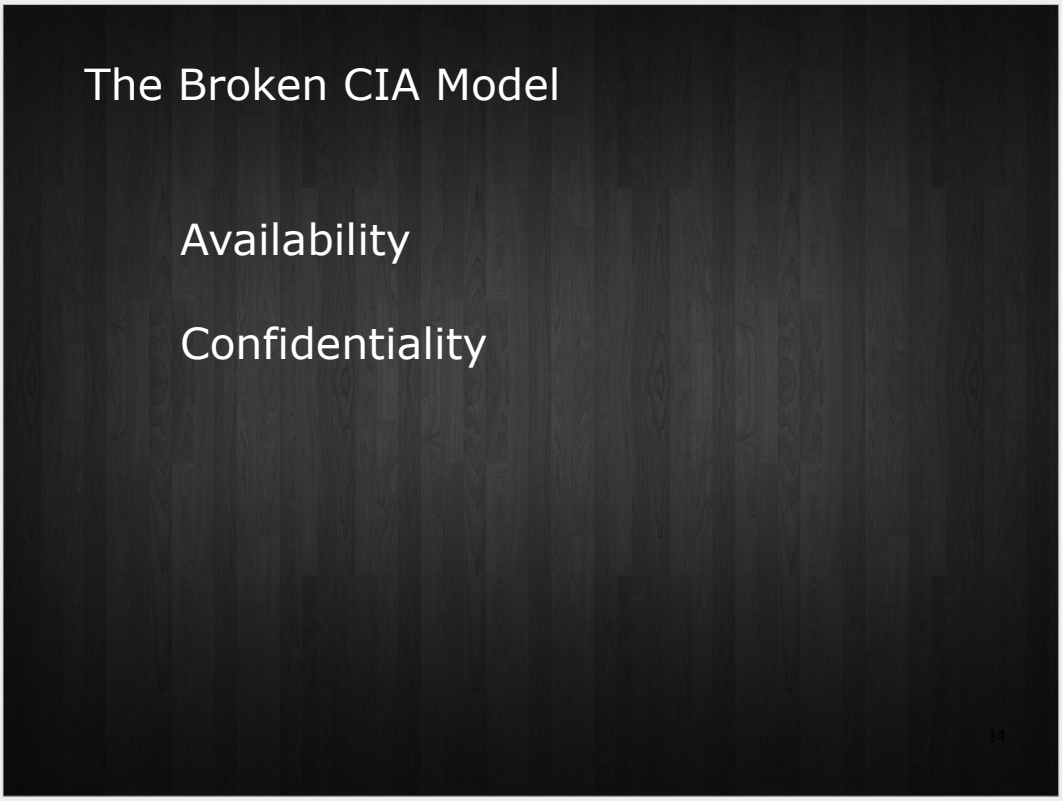
This has nothing to do with the Central Intelligence Agency.

This is the model that states information security is about protecting the confidentiality, integrity and availability of data.

The problem becomes apparent when you prioritize them.



Availability is our top priority not because it is the most important but because it is the easiest to do. Even your idiot end users can tell when a phone line or a web site isn't working. You can usually even automate the monitoring of services so you get a nice email message whenever something goes down.



This is where things start falling apart.

A breach in confidentiality simply means that someone has seen data they were not supposed to, and this is impossible for an outsider to observe as it occurs. So while there are things we can do to improve confidentiality there is no way to detect an incident which is a significant handicap.

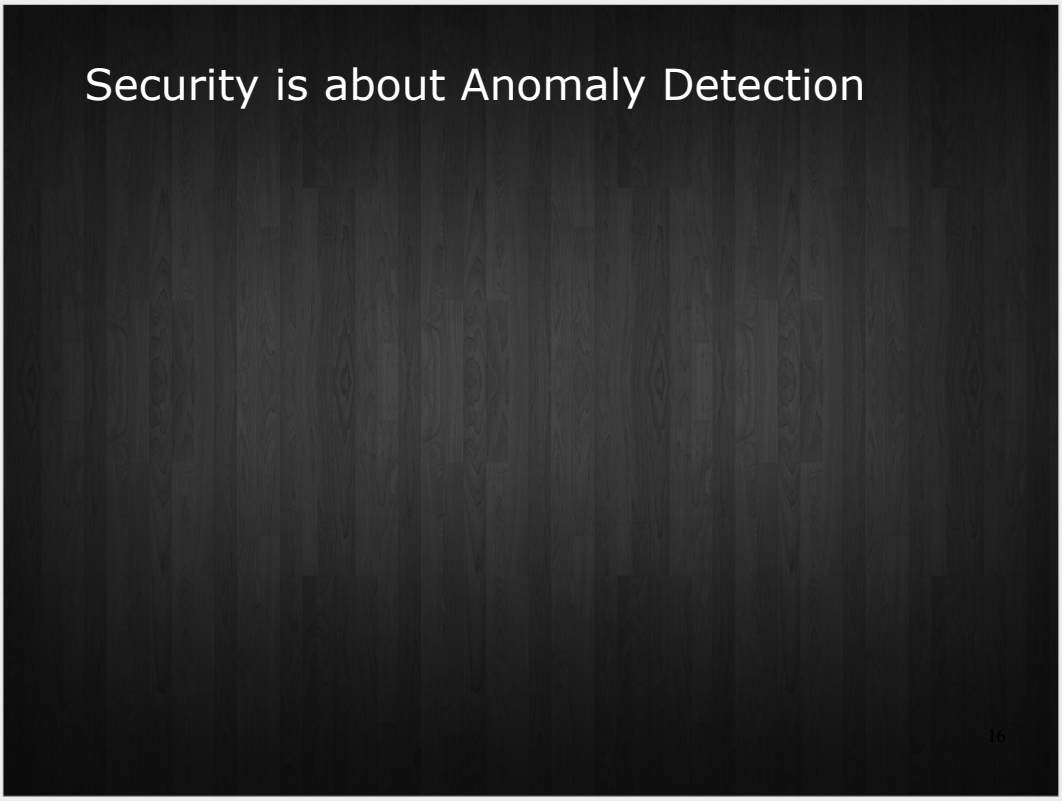
Credit cards are a great example. People seldom get caught in the act of stealing a credit card number because their behavior often appears normal. You can't tell there is a problem until you find an unauthorized purchase on your monthly statement but at that point it is too late.

Integrity is last because it is even more difficult than confidentiality.

If I have a database that is constantly being used, how can I tell if a record has been maliciously altered? I can't, so here again I have no way of detecting incidents.

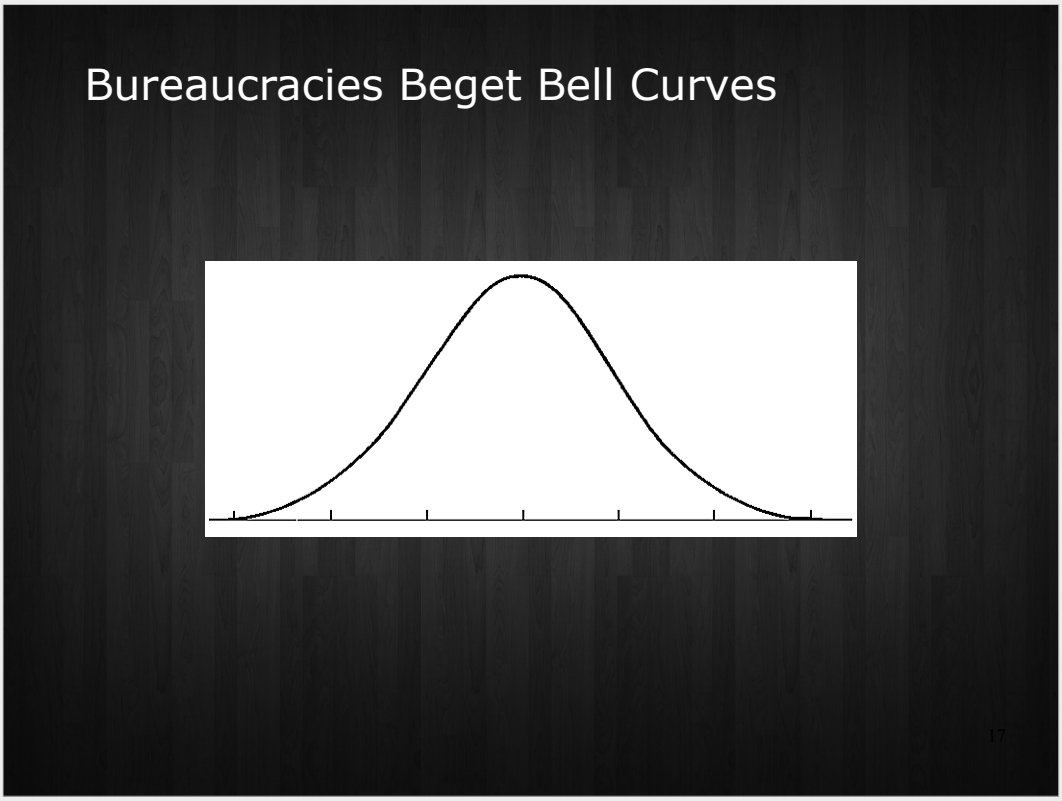
So how can we say security professionals are responsible for these three things if we can't really do two of them?

That is it for the stuff you may already know (but is wrong). Now I would like to move to concepts that you may not know.



Security is largely based on anomaly detection. This means that you need to know what something “good” looks like and what something “bad” looks like, and the more differences there are between the two the easier it will be to secure things.

This also means that if there are no anomalies then you won't be able to secure it. If a terrorist looks exactly like everyone else at the time they board a plane then you won't be able to catch him by screening passengers. You need to look in other areas where there are anomalies you can find.



Bureaucracies tend to average things out. So it doesn't matter what we are talking about: the spending of tax dollars, the effectiveness of your firewall, or employee happiness. If we are talking about a bureaucracy then we are talking about bell curves.

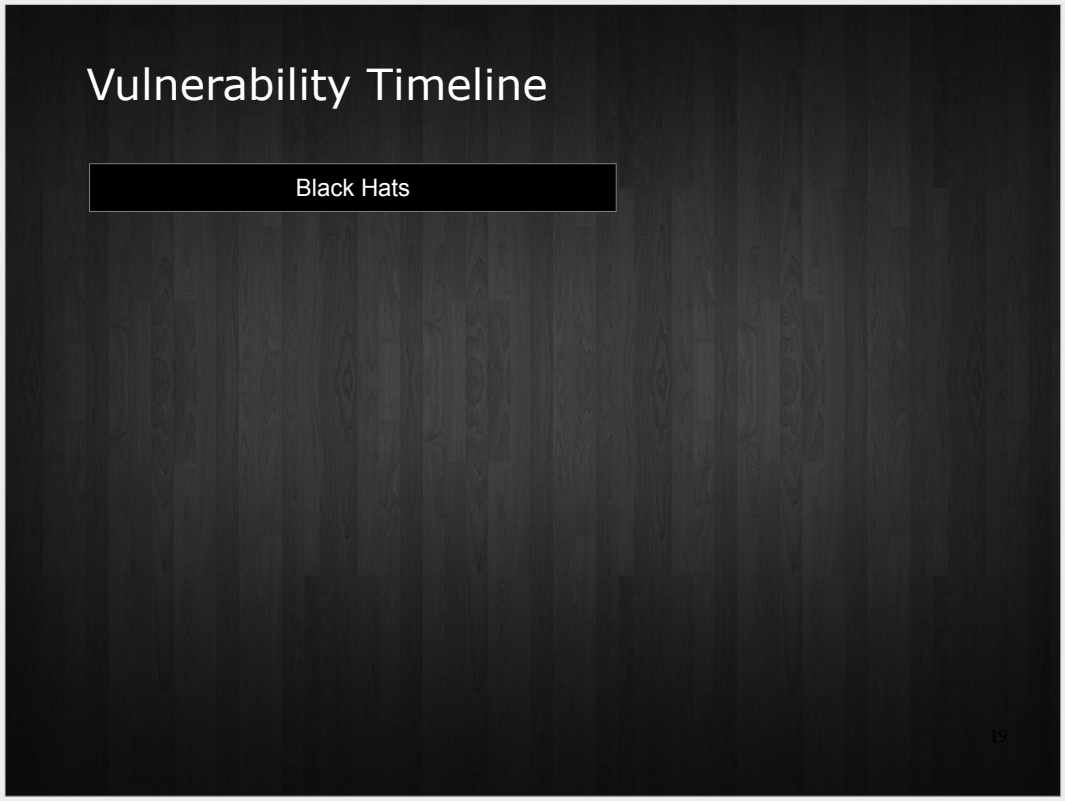
Much of the time this works pretty well. If you have crazy left-wingers on one side and crazy right-wingers on the other then you probably don't want either of them having their way. So the right answer probably lies somewhere between them. But what if one of them actually has the right answer?

Or what if your bureaucracy is trying to do things like design security controls? If one side is the worst solution and the other is the best solution then a bureaucracy will virtually guarantee you will never have the best solution.

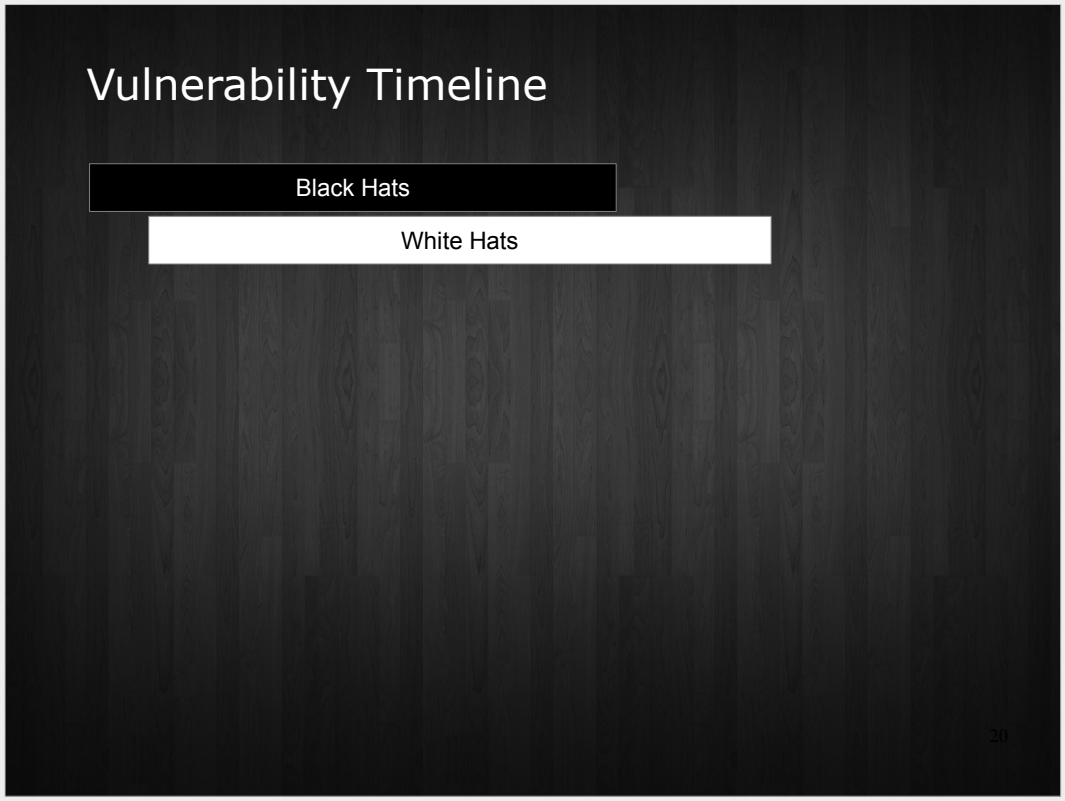
In cases where you absolutely must have the best solution then your processes must be more totalitarian. You need to reduce the number of people who can influence the decision, possibly down to a single person.

Different people discover vulnerabilities at different times, and they are concerned about them for differing lengths of time. When it comes to information technology there is also a fairly consistent order. So let's see what we can learn based solely on who knows what and when.

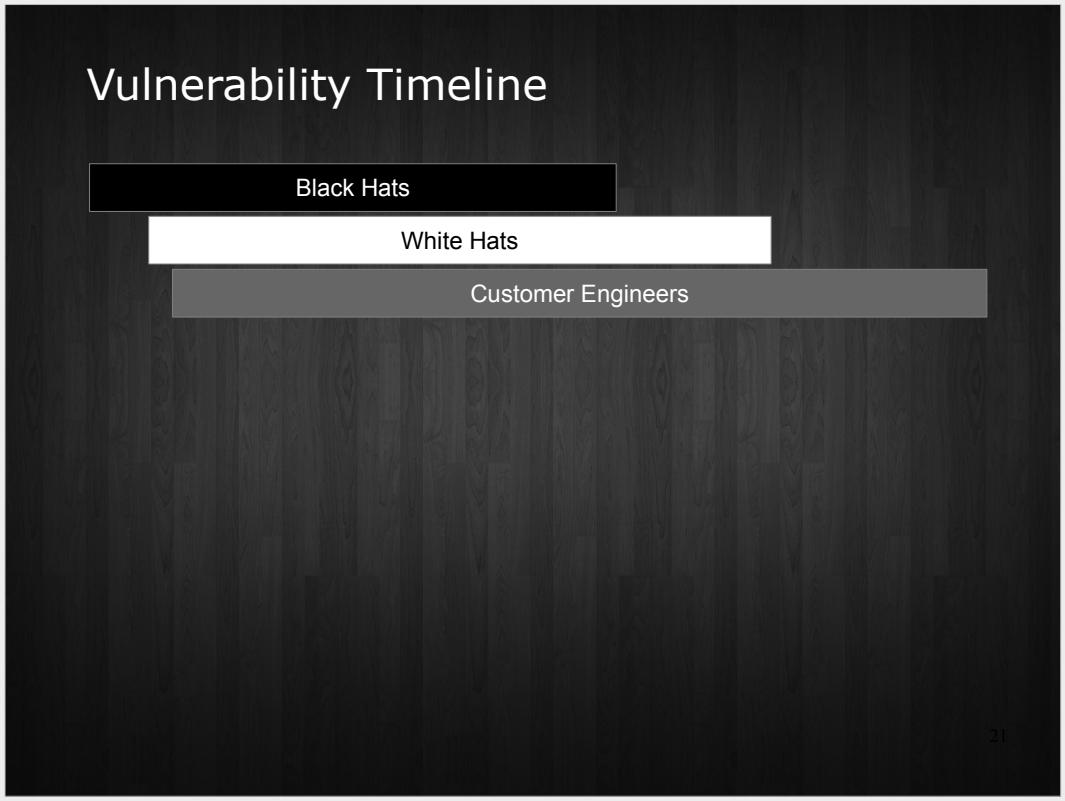
Note that theoretically anyone can discover a vulnerability at any time, but what follows is my interpretation of what I have seen in the real world.



Black hats are usually full time criminals. They will always find vulnerabilities first because they are financially motivated to discover them. If they can exploit a system in a way that no one else knows about then they may be able to use the method for a very long time.

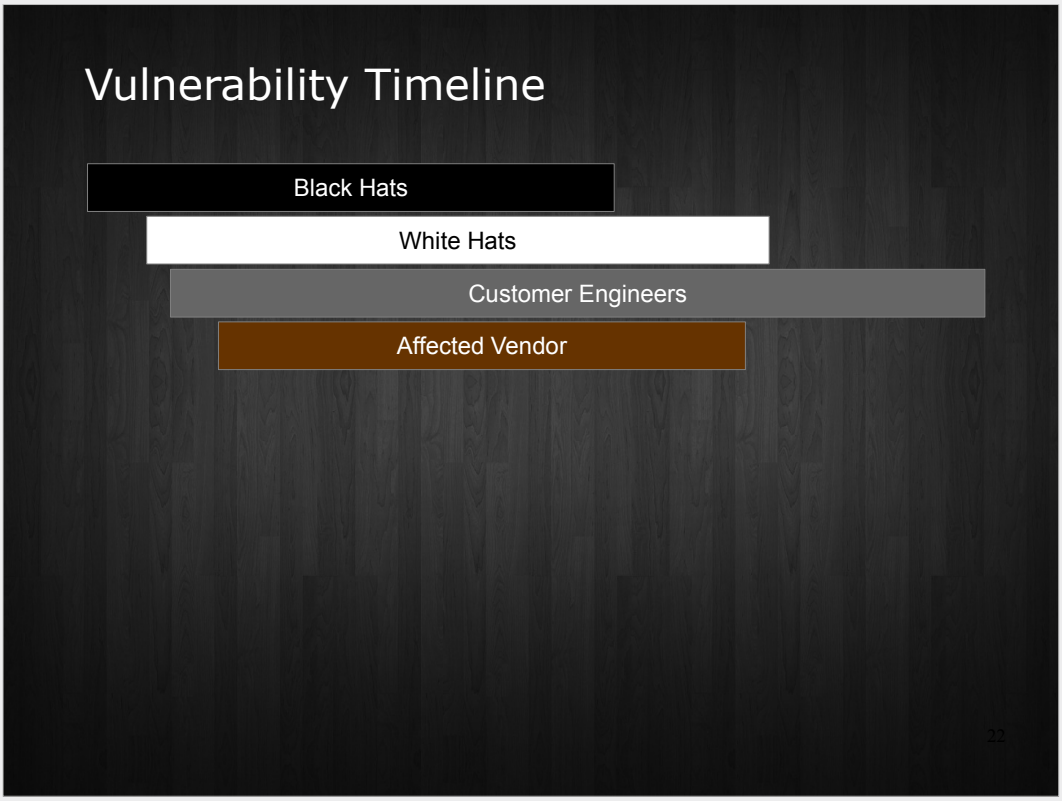


White hats also do a lot of vulnerability research but they have day jobs. Even if their job involves looking for vulnerabilities they never get paid as much as black hats because they are simply drawing a salary instead of exploiting the vulnerability in a way that steals from others. And less money = less motivation, so white hats will seldom be as “leet” as black hats.

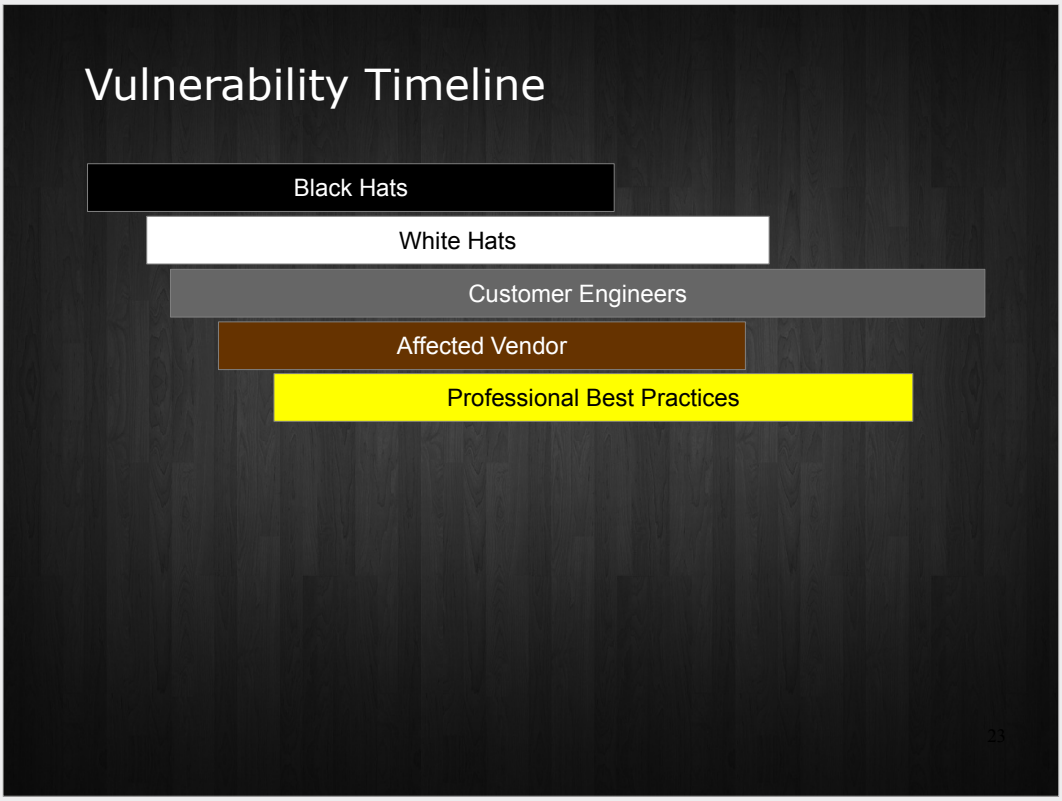


Customer engineers are usually the next to discover vulnerabilities, not because they are actively looking for them but because they often “trip over” them during the implementation of a given product.

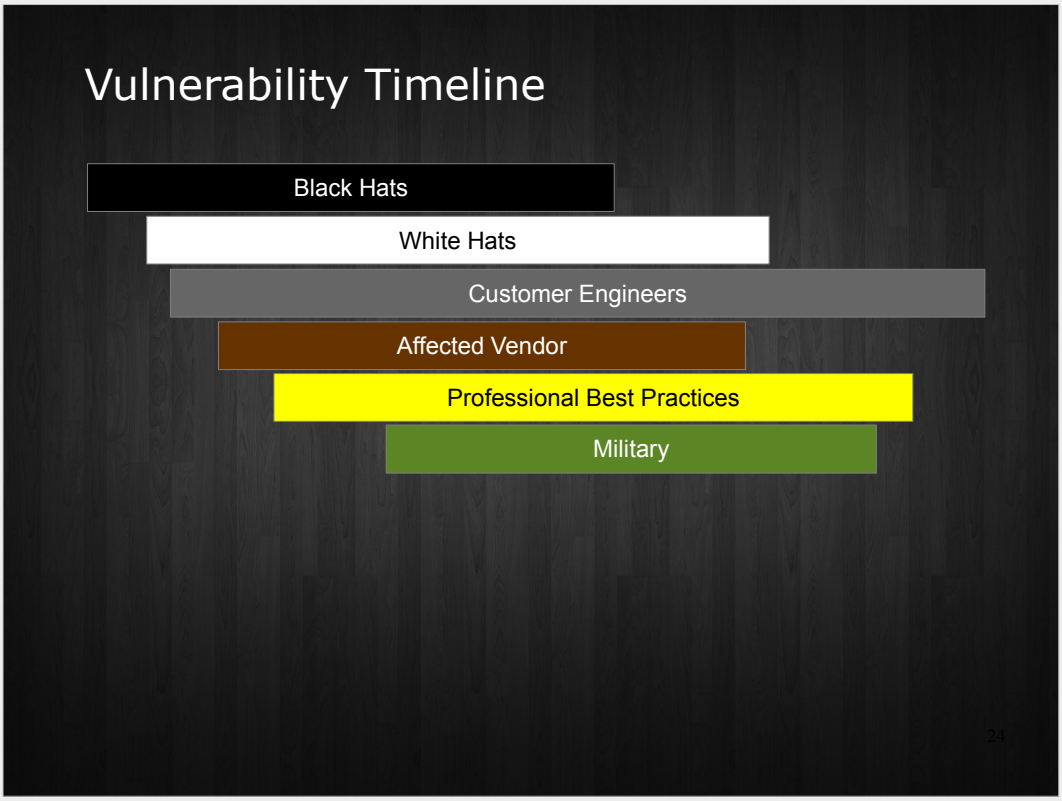
They typically care about the vulnerability for the longest period of time because they are responsible for the system until it is retired.



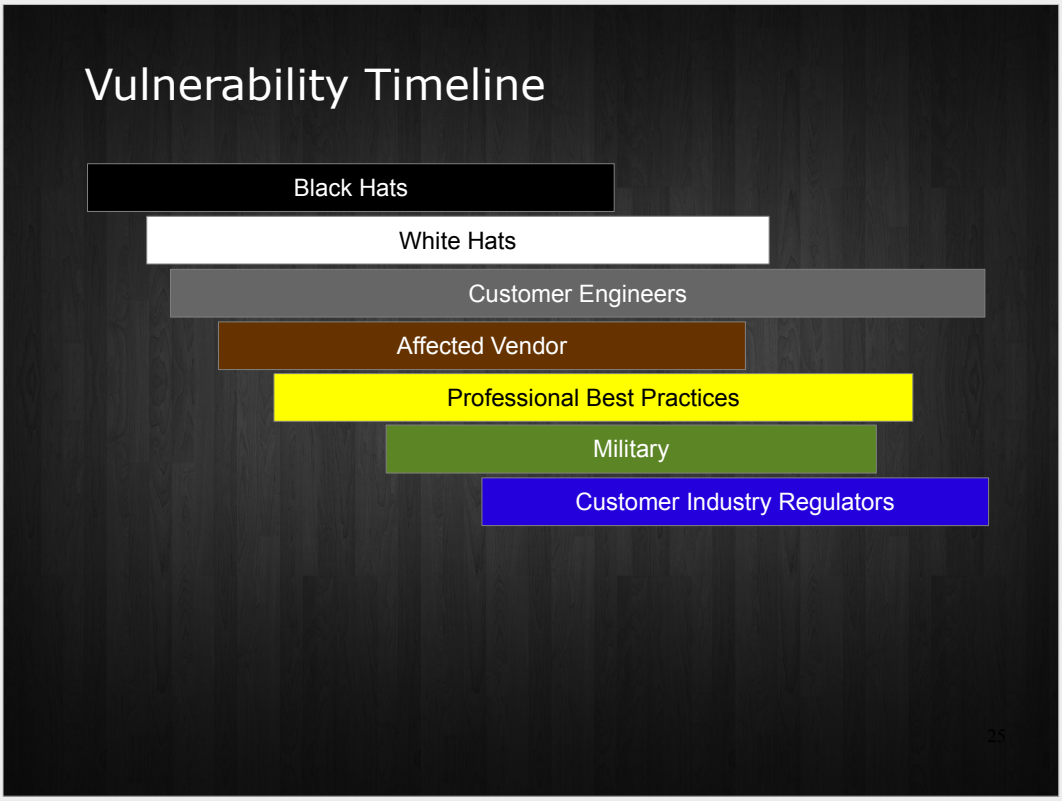
An affected vendor often discovers a vulnerability when they are yelled at by the previous two groups to fix it. They often refuse to look for the problems in advance because it simply costs too much money. But in their defense this is how security works for most industries. We don't start looking for people wearing explosive underwear until we witness someone trying to detonate them.



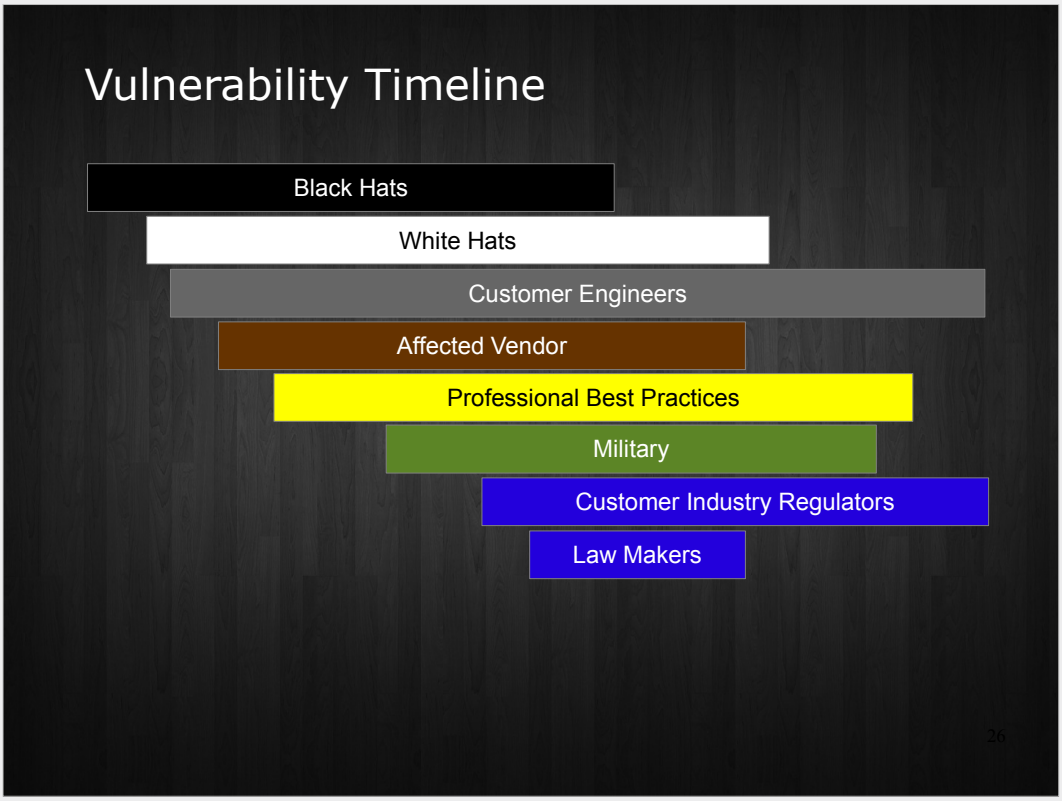
At this point patches and workarounds have been developed so industries can use their best practices to mitigate the risks associated with a vulnerability.



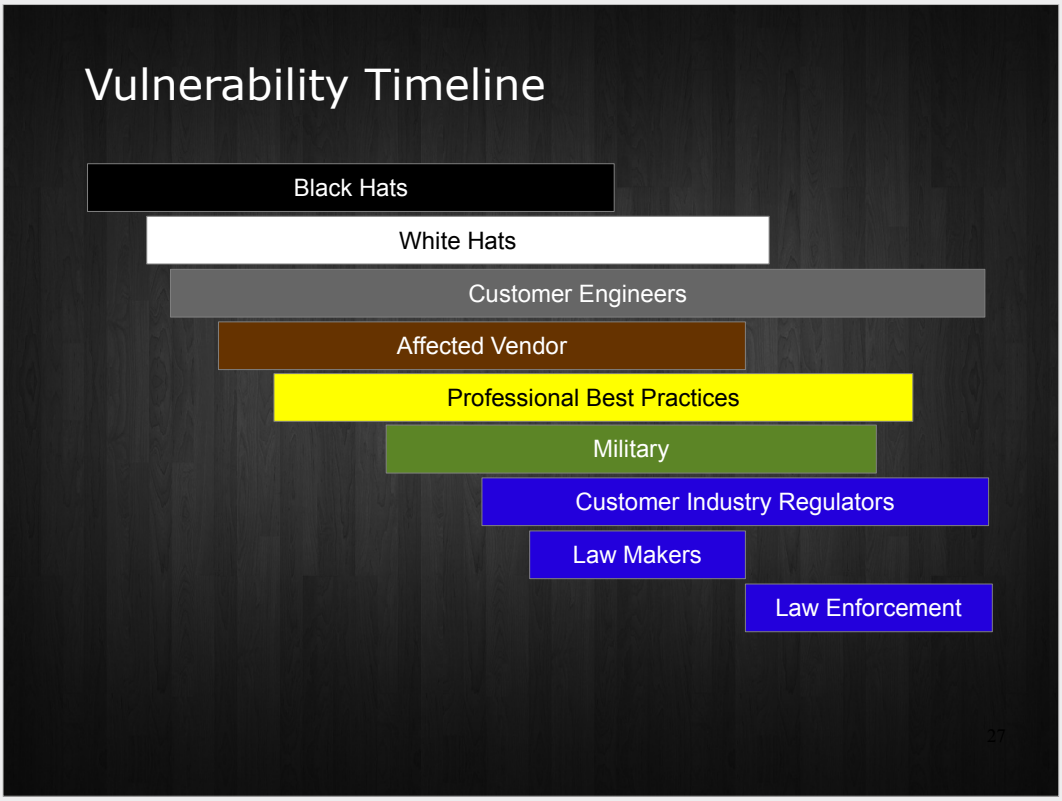
The military usually falls somewhere around here, not because they aren't intelligent but because of turnover. Since they tend to hire young people who leave just as they start getting smart I can't see how they will ever possess the wisdom required to consistently discover new vulnerabilities.



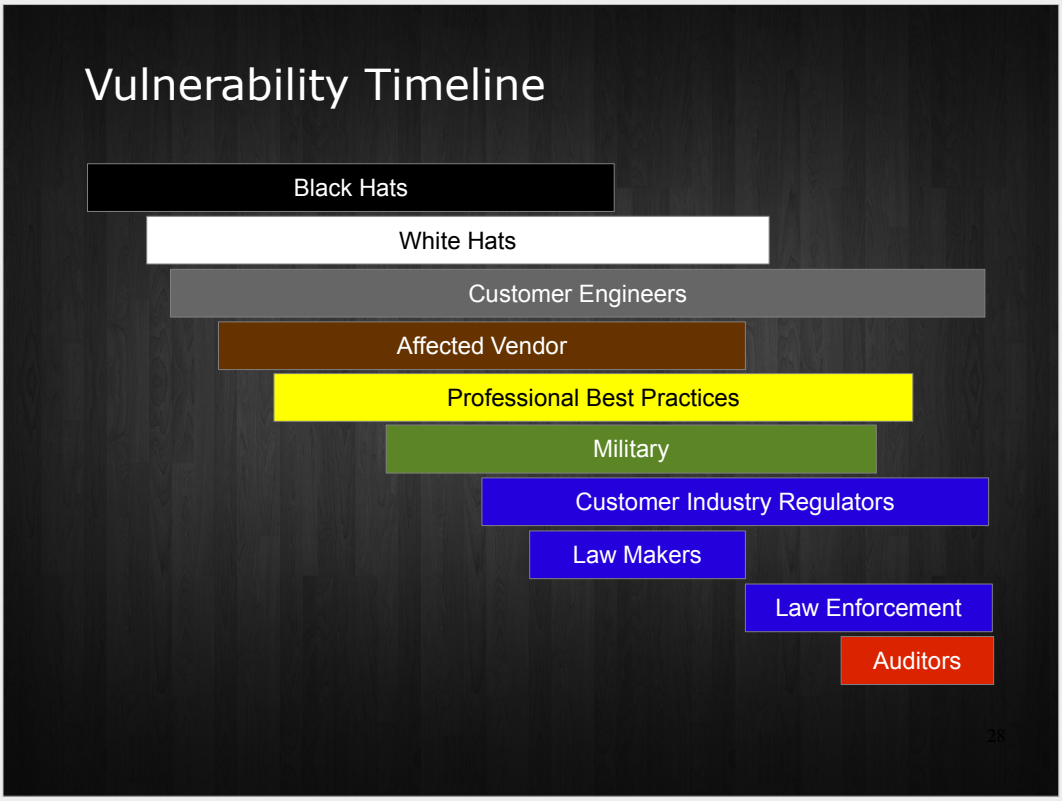
If a vulnerability goes this long without being addressed then regulators must step in to force people to do the right thing.



If things still do not get addressed then laws are created to address the issue.



It is only after laws are created that law enforcement can do something about the vulnerability.



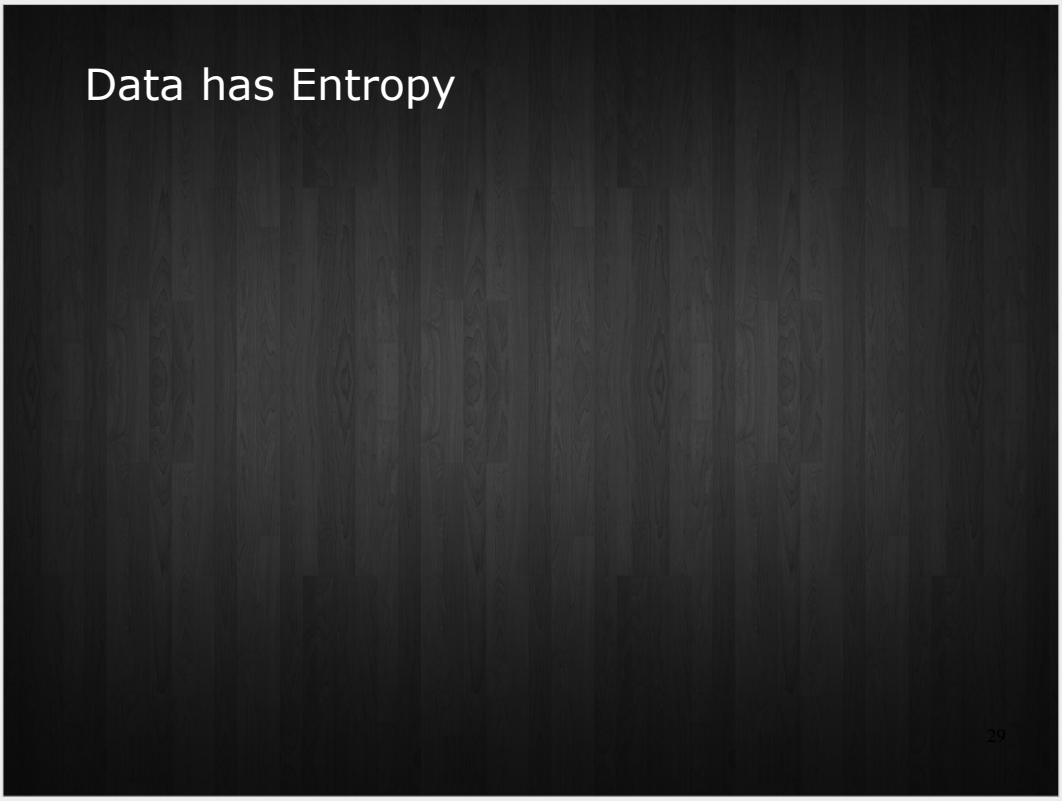
Auditors are almost always last, presumably because they don't find out about a vulnerability until they see people getting arrested on the news.

So what else does all of this tell us?

Law enforcement can never defeat black hats, once again not due to ignorance but because they are the wrong tool for the job.

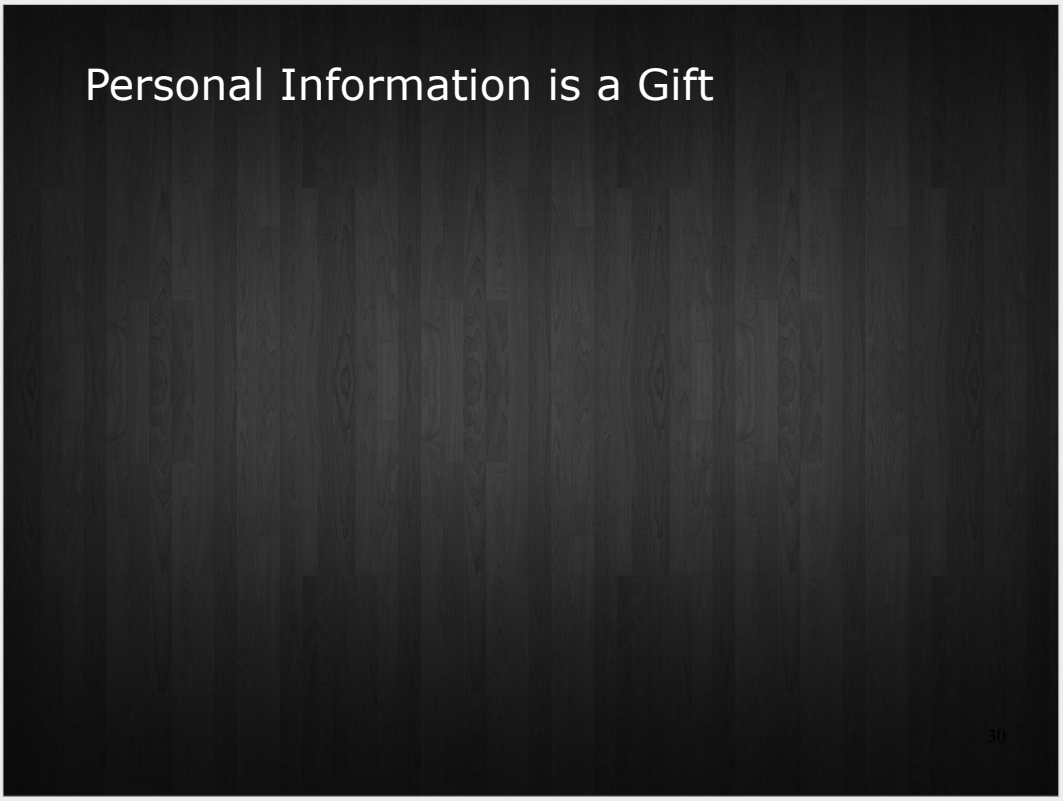
Most of the groups only react to known issues. If you discover a new method of attack most of the world will be defenseless.

There are a lot of companies that will do nothing until an auditor forces them to fix a problem. That means there are a lot of groups who know the company's vulnerabilities and who are free to exploit them whenever they'd like. What's absurd is that by the time such a company fixes a given vulnerability the direct threat is gone since the black hats are no longer interested in it.

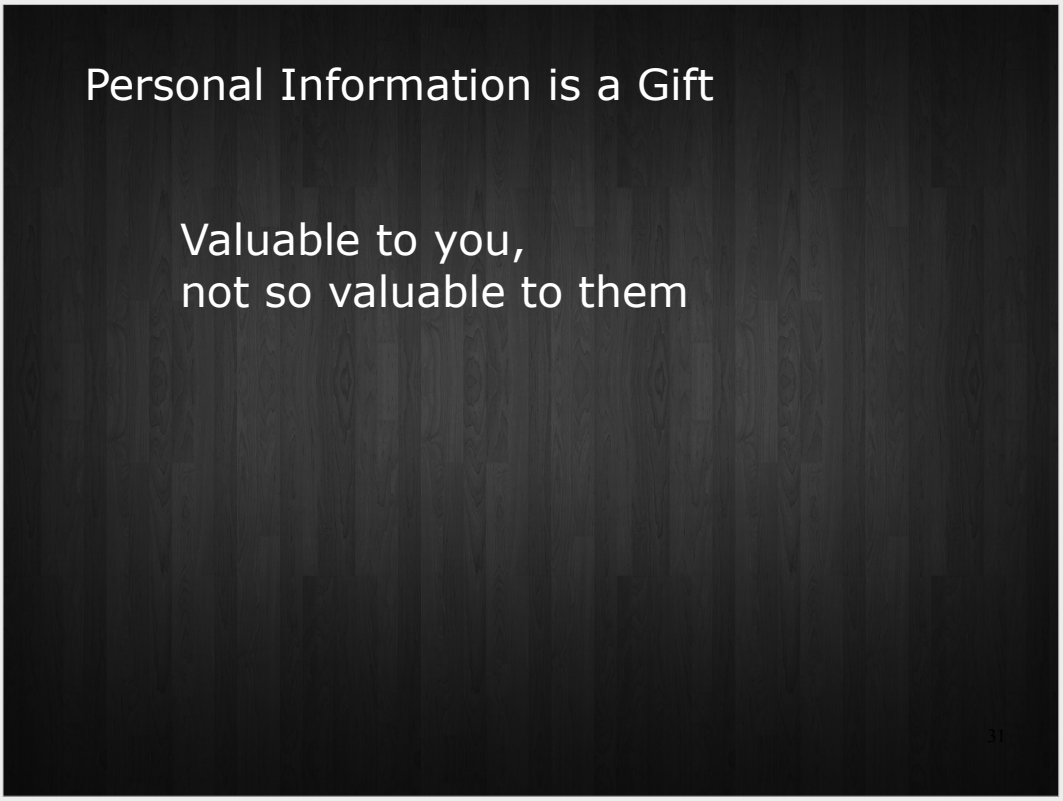


In physics the definition of entropy is: “The longer something exists the less capable it is of doing work”. For example, a star is always in the process of burning out.

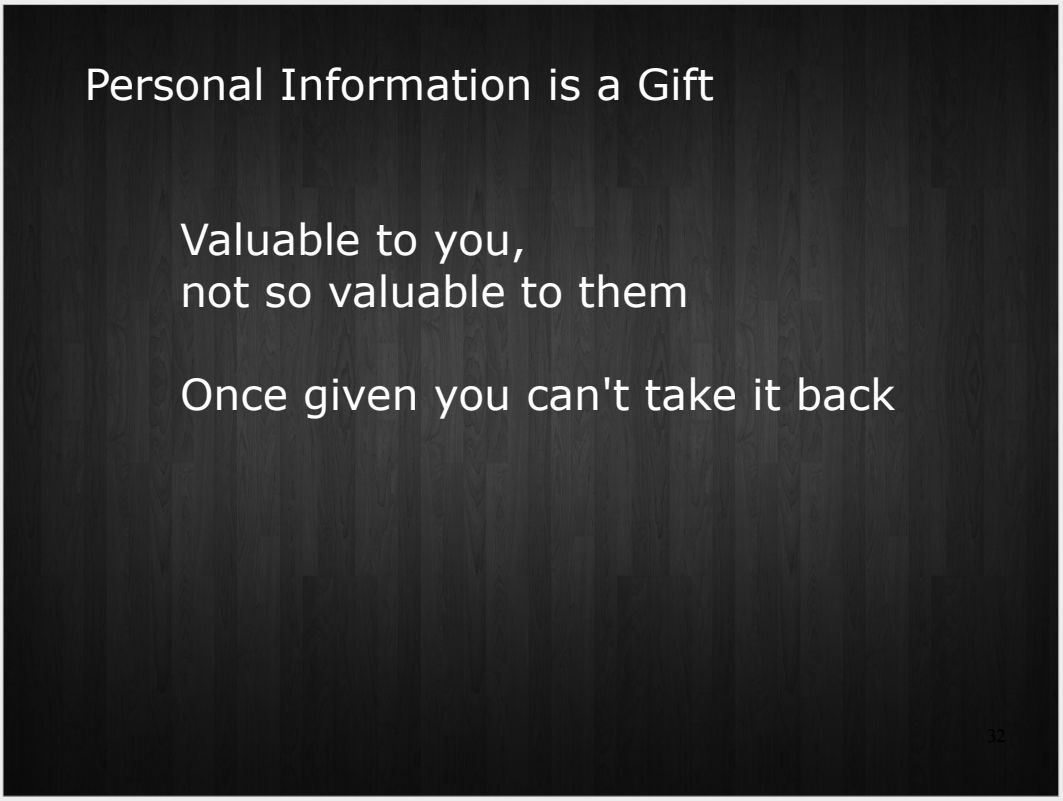
Data has the same problem. The longer data exists the less valuable it is to us, and when something becomes less valuable we don't protect it as well. But the fact that the data is worth little to us doesn't mean it's not valuable to someone else. So if your attacker does nothing more than wait they may be able to get the data they are looking for after you relax your security controls. This is why dumpster diving still works.



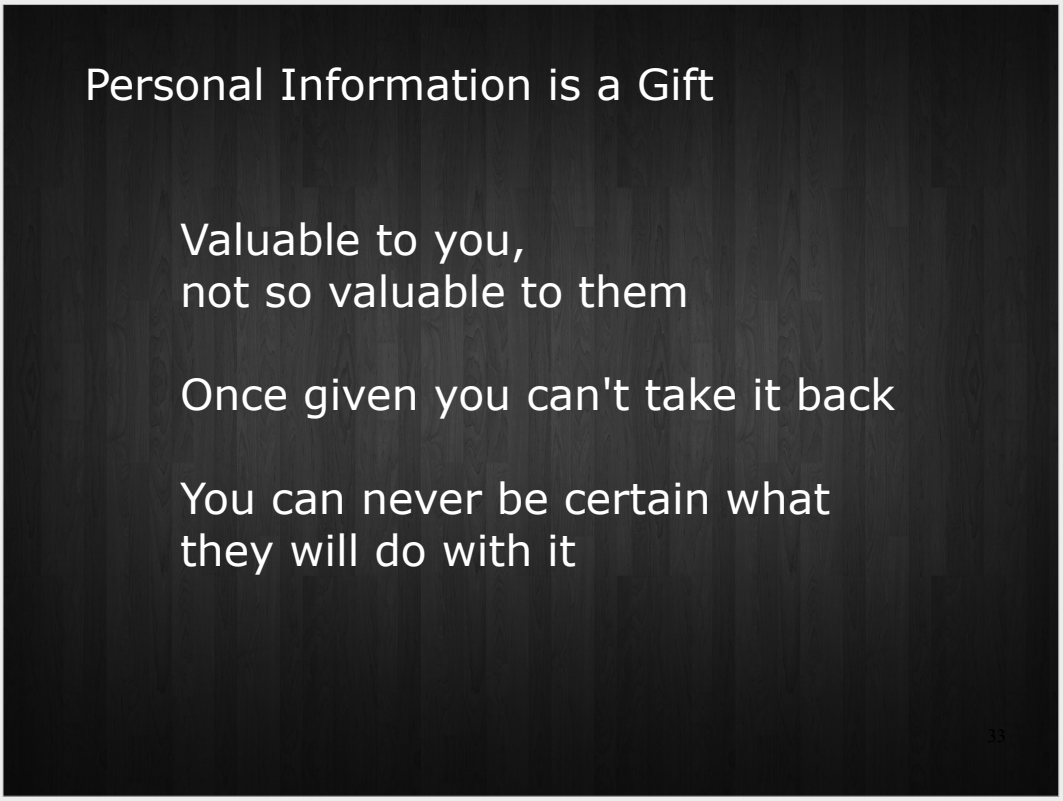
Personal information is not an asset that you own and can protect. It is a gift that you knowingly give away. And like a gift:



You are painfully aware of the value of the gift because you effectively paid for it. But the recipient doesn't value it as much as you do because it didn't cost them anything.



Once it is given it is gone – you can't unring a bell.



You have no idea what they will really do with it after you give it to them. They may say they will never sell your information to someone else but there is no way for you to verify that they don't. And if they can make money from the gift of your personal information and there is no way they can get caught, why wouldn't they sell it?

So just like a gift you had better really like who you are giving your personal information to. Don't just give it away to whoever asks for it.

The next few concepts are best described as inequalities. For example,

Frequency does not equal credibility.

If a specific Google query generates 2 million hits that does not mean the information is true.

Likewise, if a news anchor repeats the same thing over and over again that does not make their story real.

Correlation does not equal causality.

The fact that two things occurred at the same time does not mean that one caused the other, regardless of what Fox News says.

This is very important when you are doing things like looking through event logs.

Possibility does not equal probability.

The fact that something could occur does not mean it is likely to occur.

The TSA is just one example of how weird people get on this one. Believe it or not the banning of nail clippers would not have prevented 9/11.

Activity does not equal productivity.

You may be thinking, “What does productivity have to do with security?”. This is actually a great way for social engineers to find weak targets.

Think of someone you know who is frantically busy all of the time, yet who produces nothing that is practical or useful. Does that person have a good understanding of security concepts?

It has been my experience that those who are good at security are also good at criticizing themselves. This means that one can not be good at security if they are unable to comprehend that they waste time for a living. In fact I often find that those who are energetically unproductive are completely untrainable from a security perspective.

Feelings are not facts.

The next time you hear a news story, ask yourself, “Did a reliable source actually see this happen?”. You will find that much of what is in the news is actually opinion or speculation – which are not reality.

When they say, “We surveyed a thousand people and they said malware is going to be a big threat” it means absolutely nothing. Who says the people they surveyed even know what they are talking about?

You must be very careful when you expose yourself to things like journalists who speculate about what politicians might do. Your brain has a finite capacity and if you choose to fill it with things that are not real then you must expect to be delusional.

I would like to leave you with a very cool shortcut.

People don't deal with change very well, but as we know the world is constantly changing. So how do you deal with changes that affect security after something has already been deployed?

We begin by assuming your current security controls are correct. After all, if you really needed something else then you would have purchased it already, right?

Next you simply have to watch for the four things that are inversely proportional to security. If you see any of them increase then you know your security posture will weaken, therefore you will need to develop some means of mitigating the additional risk.

If you take something and make it more complex it will be less secure. Phones are one example.

Back when phones had physical wires and one company owned everything they were somewhat secure (considering they had no authentication).

Now things are wireless. And we use devices and networks owned by dozens of companies located in different countries. And every one of those companies have their own employees and their own security problems.

And phones don't just dial other phones now, either. They have GPS, SMS, email, web browsing... all kinds of stuff. So today there are exponentially more ways for an attacker to break the system.

Note that this process is not linear. If you add 50% more lines of code to an application it will not necessarily be 50% less secure, but it will be worse than what you started with.

Change tends to relax security controls.

For example, when you migrate from one system to another a snapshot of your data might end up on something like a flash drive.

Or if you replace an employee that has worked for you a long time with one who hasn't, the new employee will be more ignorant of your processes.

Predictable behavior obviously makes it easier to plan attacks against you, but you have to be careful. People are quite bad at being unpredictable. If you take a different way to work each day as a security measure then you are still behaving predictably. If I see you taking a specific path to work today I know you will not be taking that path tomorrow.

If you are responsible for something but when you really screw up nothing happens, then you are not accountable. And when people are not accountable they tend to “cut corners” which causes security problems.

This is why it is impossible to secure our infrastructure. If you read your agreement with nearly any technology provider you will find they are accountable for very little.

So always look for an increase in these four things since they indicate your overall security is getting worse.

Thanks for your time.

If you have something nice to say email particle.bored@kgb.to.