**DISCUSSION BOARD 2:**

1.) There are a lot of things to compare and contrast between IPV4 and IPV6

Address Length:

IPV6 uses a 128-bit address which allows for an extremely large amount of addresses that are unique. Right around 340 Undecillion

IPV4 uses a 32-bit address which only allows for around 4.3 billion unique addresses which we as a global population have already used. It is only still usable due to techniques such as Network Address Translation (NAT) which allows for us to use the same addresses over an over on private networks.

Address notation

IPV6 addresses are written in hexadecimal format with 8 groups of four characters such as 2001:Odb8:85f3:0000:0000:8a2e:0370:7334

IPV4 addresses are written in decimal format with four sets of numbers like 192.198.0.1

Auto-configuration:

IPV6 addresses support the ability for a device to auto-configure itself based on the prefixes of the network that it finds itself on, which makes set up a bit simpler in theory.

IPV4 address do not support auto-configuration and have to be set up manually or through a DHCP server.

Built in security:

IPV6 has IPsec built into it, greatly improving security at the network layer

IPV4 did not have security built in but it can have things like IPsec added to it.

2.) I believe that IPV4 will still be in use for a lot of the foreseeable future either due to the cost of upgrading to IPV6 compatible hardware or just some hold outs that don~~t want to change. I also believe that IPV6 is being steadily adopted but not at an extremely rapid rate. I am not currently employed but when I left the army they were starting to convert to IPV6 but it wasnt wide spread at that point yet.~~

~~3.) There are a lot of things that would have to change in order for UDP to take over for TCP. TCP is is a reliable, and secure protocol that has been widely adopted into the applications and networks worldwide. In order to switch over to UDP the protocol would have to be optimized performance and security wise, as far as I understand it is mainly used in situations where you want low latency. It would have to see widespread adoption, network admins would have to be trained in the best practices of the use of UDP and network hardware would have need to be able to effectively use UDP for things like Quality of Service (QoS) on the network which would likely require a little bit more development.~~

**DISCUSSION BOARD 3:**

There are so many things that you can implement to implement a Data Loss Prevention program and prevent sensitive data from “walking away.” I will list a few so that maybe all of us don’t create the same list.   
The most important that I can think of is user education and access control, I believe that most of the time sensitive information leaks are not done maliciously they are done for the sake of convenience or ignorance. If the users do not know how to protect the data or what could happen if that data gets out, then they are at a disadvantage when it comes to protecting said data. Access control is also vital in that if a user does not have a need for certain data they they should not have access to it, access controls tend to get circumvented by possibly overworked, lazy or improperly trained admins as they either don’t do periodic reviews (possibly due to the volume of work) of what each user has access too or do not know the ramifications of giving their friend access to “everything.”   
Encryption and endpoint security are two more things that are very important in my mind. Encryption refers to both data at rest and data on the move for the most part I am thinking more about the data at rest, this would particularly help if say a laptop or something was stolen. While it is not impossible to crack the encryption the thief would have to work very hard for that data which most of the time is not really worth the effort as by the time you get through the encryption the data is stale. When I speak of end point security I am thinking more of preventing the usage of USB drives or to restrict the copying of sensitive files to external storage. Though there are many other things you can do in these two areas alone.   
Data loss is constantly moving target in that as we develop strategies to secure the data the bad actors are devising ways to get around those strategies. So, the cycle continues and does not end. So it is in our best interest to continuously continue to evolve in or efforts.

**DISCUSSION BOARD 4:**

1.) Is one type of application technology or architecture more secure than another? Why or why not?

For the most part and application technology’s security isn’t determined by the technology alone but on a lot of factors such as implementation, configuration, and maintenance. Though there are some technologies that are considered more secure than others such as Static websites and blockchain technology. Static websites are considered more secure due to most of the data staying the same and there not being very much input / output from the site therefore reducing it’s attack surface. Blockchain is also considered more secure due to dispersed nature of it’s architecture.

2.) Can code reviews or source code analyzers identify all types of vulnerabilities in software?

The short answer to this question is no code reviews and code analyzers can not identify all types of vulnerabilities. These tools are very good at detecting known vulnerabilities such as SQL injections or XSS attack vulnerabilities but could and would probably miss vulnerabilities that are related to application specific security requirements or vulnerabilities that only appear when the program runs

3.) Research and report on three different source code analyzers and their efficacy.

Three different source code analyzers that I looked up were:

SonarQube: This analyzer scans your code as you develop it to assist you as a developer to use good coding practices and helps to raise the over all quality of your code. The effectiveness would probably depend heavily on what rules and plugins you had turned on in the analyzer.

Checkmarx: This tool allows you to scan un-compiled code to check for security vulnerabilities in most of the popular coding languages. This one will provide detailed reports and integrates with most popular development environments. What I read said that it was very effective at identifying complex vulnerabilities.

Fortify: This tool is a suite of analyzers for many different programming languages and many different frameworks so this would be effective to use on mobile apps, containers, and web apps to name a few. What I read said that fortify tends to focus on security vulnerabilities and compliance problems and is also said that it has a strong reputation for in-depth static analysis which unfortunately did not help me in determining how effective it might be.

**Discussion Board 5:**

When would a quantitative risk assessment be favored over a qualitative risk assessment?

You would prefer a quantitative risk assessment when you have good amount of historical data give you a more detailed understanding of the probability of the event occurring and the potential losses from such an occurrence happening.

What might be some of the challenges of an information classification program?

The ones I can think of are scope, integration, and user compliance. Scope can be an issue because trying to determine what gets classified can be a challenge and there is always the possibility of going too far, which would make your employees jobs difficult or not far enough in which case you miss classifying data that you should be classifying. Integration can be difficult to work into existing workflows and user compliance kind of runs hand in hand with the integration. If your classification system makes it difficult for the employees to do their jobs, you will have to pay close attention to your workers to ensure that they are classifying and handling classified materials correctly.

What are some key factors in mitigating risk?

Backups and redundancies are one key factor in mitigating risk. Others are encryption, security policies, risk assessments, access controls, and employee training.

How can an organization know whether it is compliant with its own security policies?

The main way an organization can ensure that they are compliant with their own security policies is with regular audits. Using security monitoring tools that can detect policy violations and records of security activities so that they can access their compliance and continue make improvements.

**Discussion Board 6:**

If an organization decides to no patent one of their product designs there are still other legal means that they can use to protect their trade secrets. There are actual trade secret laws though they are different depending on the jurisdiction the company is in but they are generally there to protect things such as manufacturing processes, formulas, and marketing strategies to name a few. Other things that companies can use are Non-Disclosure Agreements (NDA), and Non-compete clauses. Many companies with secrets to keep will have employees sign an NDA at the beginning of their employment and sometimes will put non-compete clauses into their contracts to protect against their trade secrets either being disclosed to the competition or being used against them by prior employees.

The main concerns of citizens today in regards to privacy in information systems would be Data breaches, Surveillance, and Lack of control. There have been a lot of data breaches that have exposed vast amounts of personal data. Which has fed into the peoples concerns about the lack of control that they have over how their data is collected and used by corporations and governments without their consent. Which kind of feeds into their worry about corporations and governments doing surveillance on their everyday digital lives.

Three vulnerability assessment tools that are in use by medium to large businesses today are:

Nessus – this application is a widely used vulnerability assessment tool that scans networks, systems and applications for security vulnerabilities. Its main features are that it has an extensive vulnerability database and it integrates with other security tools and has good reporting capabilities. I could not find much on the cost for commercial use but there is a free trial avaliable.

OpenVAS – or Open Vulnerability Assessment is a pretty popular open source vulnerability scanner. Its primary features are a database that is updated regularly, scripting support, and a user friendly interface. This tool is open source so therefore free to use.

Qualys Vulnerability Management – This is a cloud based vulnerability management tool that assists organizations to identify, prioritize, and fix their security vulnerabilities. The man features are that it offers continuous monitoring, asset discovery and a comprehensive reporting system. This tool is paid for by a subscription based model.

**Discussion Board 7:**

I think that the first thing that I would end up doing would be to shifting my auditing efforts to a more risk based approach. By identifying the companies critical data and points of interest I would then be able to start to focus my efforts into our high risk areas.

I would then want to to automate the Vulnerability scanning and Log analysis, if I automate the vulnerability scanning then I can set the scanner to flag medium to high risk vulnerabilities that were found for further analysis by a human, therefore limiting the magnitude of data that the auditor has to sift through. The automation of the log analysis would basically be for the same reason, configure the software to flag probable issues in the security logs so that the auditor is not sifting through reams of data.

I would automate the user and access management portion of the system making it so that if a user is say promoted or laterally moved they have the proper permissions for the job that they are doing and if they get fired or quit then they are removed from the system with as little needed input from the system administrators as possible so that there are no potential vectors for the a threat agent to target while the administrators slog through their back log of work. There are more things that you can do to help automate the audit process but I figured that I would only tag a few so that we are, hopefully, not all talking about the same exact thing.

**Discussion Board 8:**

You can use data replication as a form of data backup but it not always the best way to do data backups. Primarily there are two reasons why this would not be the best way. One would be that any errors or corruptions that happen in the source data would be instantly mirrored in the replicated data, a better way would be to use a system to create periodic backups so that if the source data gets corrupted you would be able to use the backup to restore either the affected files or the entire file system to a point before the corruption happened to the file system. Which leads into the second one there is no historical record of the data if you use a direct replication backup method so there is no real way to see what the original data was if for instance if a malicious attack changed your companies’ data.

Computer forensic experts face many challenges. The increase in the use of encryption to keep our data safe presents some interesting challenges for forensic experts in that some or all of the data may be inaccessible without the appropriate decryption keys. Jurisdictional issues, and vastly different levels of technical expertise among the different agencies could be a challenge that today’s computer forensic experts have to face. With DoJ involvement the forensics experts face challenges with getting warrants, handling privacy issues and making sure that the chain of custody and protocols for handling digital evidence are adhered to in order to assure that the evidence that they gather is admissible in a court of law.

Three information gathering tools for court admissible evidence are:

EnCase Forensic – which allows investigators to gather and preserve electronic forensic evidence. It follows the guidelines put down by HTCIA and provides features make sure that the evidence is handled in forensically sound manner.

Autopsy: this is a forensic tool kit that allows for both a command line and graphical user interface which is made possible because Autopsy is laid out over and interfaces with it’s predecessor called Sleuth Kit. This software is user friendly and meet the standards for court admissible digital evidence.

SIFT (SANS Investigative Forensic Toolkit) – is a Linux opensource toolkit developed by SANS that features a wide array of tools for forensic analysis, evidence gathering, and documentation of said evidence in a manner admissible in a court.