- Vulnerability Types
    - Zero day attacks
        - Many applications have vulnerabilities
        - We've just not found them yet
        - Someone is working hard to find the next big vulnerability
            - The good guys share these with developers
        - Attackers keep these yet-to-be-discovered holes for themselves
            - They want to use these vulnerabilities for personal gain
        - Zero-day
            - The vulnerability has not been detected or published
            - Zero-day exploits are increasingly common
        - Common Vulnerability and Exposures
    - Open Permissions
        - Very easy to leave a door open
        - The hackers will always find it
        - Increasingly common with cloud storage
            - Statistical chance of finding an open permission
        - June 17 - 14 million Verizon records exposed
            - Third party left an Amazon S3 data repo open
            - Researcher found the data before anyone else
        - Many, many other examples
            - Secure your permissions
    - Uncensored root accounts
        - The linux root account
            - The administrator or superuser account
        - Can be a misconfiguration
            - Intentionally configuring an easy-to-hack password
            - 123456, ninja, football
        - Disable direct login to the root account
            - Use the su or sudo option
        - Protect accounts with root or administrator access
            - There should not be a lot of these
- Errors
    - Error messages can provide useful information to an attacker
        - Service type, version information, debug data
    - Sep 2015 - Patreon is compromised
        - Used a debugger to help monitor and troubleshoot web site issues
        - Was left exposed to the internet
        - Effectively allowed for remote code executions
        - Gigabytes of customer data was released online
- Weak encryption
    - Encryption protocol (AES, 3DES, etc)
        - Length of the encryption key (40 bits, 128 bits, 256 bits, etc.)
        - Hash used for the integrity check (SHA, MD5, etc)

        - Wireless encryption (WEP, WPA)
    - Some cipher suites are easier to break than others
        - Stay updated with the latest best practices
        - TLS is one of the most common issues
            - Over 300 cipher suites
    - Which are good and which are bad
        - Weak or null encryption (less than 128 bit key sizes), outdated hashes (MD5)
- Insecure protocols
    - Some protocols are not encrypted
        - All traffic sent in the clear
        - Telnet, FTP, SMTP, IMAP
    - Verify with a packet capture
        - View everything sent over the network
    - Use the encrypted versions
        - SSH, SFTP, IMAPS, etc.
- Default settings
    - Every application and network device has a default login
        - Not all of these are ever changed
        - Mirai botnet
            - Takes advantage of default configurations
            - Takes over IOT devices
            - 60+ default configurations
            - Cameras, routers, doorbells, garage door openers etc. (IoT)
        - Mirai released as open source software
            - There's a lot more where that came from
- Open ports and services
    - Services will open ports
        - Its important to manage access
    - Often managed with a firewall
        - Manage traffic flows
        - Allow or deny based on port number or application
    - Firewall rulesets can be complex
        - Its easy to make a mistake
    - Always test and audit
        - Double and triple check
- Improper Patch Management
    - Often centrally managed
        - The update server determine when you patch
        - Test all of your apps, then deploy
        - Efficiently manage bandwidth
    - Firmware
        - The BIOS of the device
    - Operating System

        - Monthly and on demand patches
    - Applications
        - Provided by the manufacturer as needed
    - Improper patch management - Equifax
        - Data breach of 147.9 million Americans, 12.2 million british citizens, 19k canadian citizens - names, ssns, birthdates, addresses
    - Apache Struts vulnerability
        - Breach started March 12
        - Wasn't patched by Equifax until July 30th after discovering sus network traffic
        - Sep 7 public disclosure
        - CIO and CSO fired from Equifax - Paid 575 million in fines
- Legacy platforms
    - Some devices remain installed for a long time
        - Perhaps too long
    - Legacy devices
        - Older operating systems, applications, middleware
    - May be running end-of-life software
        - The risk needs to be compared to the return
    - May require additional security protections
        - Additional firewall rules
        - IPS signature rules for older operating systems

- Third party risks
    - IT Security does not change because its a third party
        - There should be more security, not less
    - Always expect the worst
        - Prepare for a breach
    - Human error is still the biggest issue
        - Everyone needs to use IT security best practices
    - All security is important
        - Physical security and cyber security work hand in hand
- System integration risk
    - Professional installation and maintenance
        - Call include elevated OS access
    - Can be on site
        - With physical or virtual access to data and systems
        - Keylogger installations and USb flash drive transfers
    - Can run software on the internal network
        - Less security on the inside
        - Port scanners, traffic captures
        - Inject malware and spyware
            - Sometimes inadvertently
- Lack of vendor support

    - Security requires diligence
        - The potential for a vulnerability is always there
    - Vendors are the only ones who can fix their products
        - Assuming they know about the problem
        - And care about fixing it
    - Trane ComfortLink 2 thermostats
        - Control the temperature from your phone
        - Trane notified of three vulnerabilities in April 2014
        - Two patched in April 2015, one in Jan 2016
- Supply chain risk
    - You can't always control security at a third party location
        - Always maintain local security controls
- Hardware and software from a vendor can contain malware
    - Verify the security of new systems
    - Counterfeit hardware is out there
        - It looks like a Cisco switch…
        - Is it malicious?
- Outsourced code development
    - Accessing the code base
        - Internal access over a VPN
        - Cloud-based access
    - Verify security to other systems
        - The development systems should be isolated
    - Test the code security
        - Check for backdoors
        - Validate data protection and encryption
- Data Storage
    - Consider the type of data
        - Contact information
            - Healthcare details, financial information
        - Storage at a third party may need encryption
            - Limits exposure
                - Adds complexity
            - Transferring data
                - The entire flow needs to be encrypted channel

---

- Vulnerability Impacts
    - Malicious cyber activity cost U.S. economy between $57 billion and $109 billion in 2016
        - The cost of Malicious Cyber Activity to the U.S. Economy, the council of economic advisers, feb 2018
    - Many other non-economic impacts
        - Fear reaching effects
    - These are the reasons we patch vulnerabilities

- Data Loss
    - Vulnerability: Unsecured databases
        - No password or default password
    - July 2020 - Internet facing databases are being deleted
        - No warning, no explanation
            - Thousands of databases are missing
            - I hope you had a backup
                - Overwrites data with iterations of the word “meow”
- Identity theft
    - May through July 2017 - Equifax
        - Data breach of 147.9 million Americans
        - Apache Struts
    - Financial Loss
        - March 2016 - Bank of Bangladesh
            - Society for Worldwide Interbank Financial Telecommunication (SWIFT)
            - Attackers sent secure messages to transfer nearly one billion dollars in reserves to accounts in Philippines and Sri Lanka
            - Thirty five requests were acted upon
                - 81 million list and laundered through Filipino casino industry
            - 12 million from Wells Fargo
            - 60 mil from Taiwanese Bank
    - Reputation Impacts
        - Getting hacked isnt a great look
            - Organizations are often required to disclose
                - Stock prices drop, at least for the short term
            - October 2016 - Uber breach
                - 25.6 million names, email addresses, mobile phone numbers
            - Did Not publicly announce it until Nov 2017
            - Allegedly paid the hackers 100k and made them sign NDA
- Availability Loss
    - Outages and downtime
        - Systems are unavailable
    - The pervasive ransomware threat
        - Brings down the largest networks
    - September 2020 - BancoEstado
    - Bank closed for an extended period