CYBER SECURITY BEST PRACTICES FOR YOUR SHOP

ASCCA CONNECTED CARS COMMITTEE

Mission Statement: *The Committee shall protect the ability of ASCCA membership to do business in California, including safe, secure, and uninterrupted access to vehicle onboard systems and the required tools to fix them.*

Committee Goals

Develop steps and procedures to provide to ASCCA members to assist them with preparing for the future of automotive repair on connected cars.

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

What the Connected Cars Committee believes is needed to maintain access to vehicle data

Prove that we have secure environments and secure tools that can gather and use that data

Fight for secure data link connections through J3138 and J3146 that allow us access

Create secure shop networks and guest networks

Make sure we have a modern router that will securely separate a guest network from a secure shop network

Maintain data backups and change passwords regularly

Be proactive not reactive to our shop's security

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

Cyber Security Myths

- “I have virus protection software so I am already secure.”
- “I have nothing to worry about; there are too many computers on the Internet for hackers to bother with mine.”
- “Network and computer security is only important for large businesses.”
- “I know what is running on my computer network and I am sure that it is secure.”
- “The best time to deal with network security is when a problem arises.”
- “ Macs don’t have problems they are more secure”

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

TeamLogicIT®

Barriers to Cyber Security

Why do I need this?

How can I do this at my shop?

How much does this cost

Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

WHY IS THIS IMPORTANT?

We need to protect or clients information:

Both personal info and vehicle info.

We need to protect our data base from:

Ransom ware

Employee Errors

Customers

Loosing our data

Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

RANSOM-WARE. WHAT IS IT?

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

RANSOM-WARE. HOW DOES IT HAPPEN TO ME?

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

Rate Of Ransomware Attacks

A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021.

1.5 million new phishing sites are created every month.

Ransomware attacks have increased over 97 percent in the past two years.

A total of 850.97 million ransomware infections were detected in 2018.

34% of businesses hit with malware took a week or more to regain access to their data.

In 2019 ransomware from phishing emails increased 109 percent over 2017.

ASCCA

Automotive Service Councils of California

Professionals in Automotive Service ~ Since 1940

www.ascca.com

Ransomware costs businesses more than $75 billion per year.

The average ransom organizations paid per incident during the first quarter of this year stands at $12,762, compared to $6,733 in the final quarter of 2018.

75% of companies infected with ransomware were running up-to-date endpoint protection

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

What about employees?

- DVI Inspection?
- Personal computer?
- Phones?
- Shop computers?
- “I was just trying to help”
- Do you have an internet policy in your shop?

Oh yea,customers.

Shop guest network:

Password protected?

Behind a firewall?

Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

87% of cars in the U.S. will be equipped with wireless technology that collects and reports on car safety, maintenance and repair by 2022.

(Auto Care Association)

ASCCA

Automotive Service Councils of California

Professionals in Automotive Service ~ Since 1940

www.ascca.com

National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333).

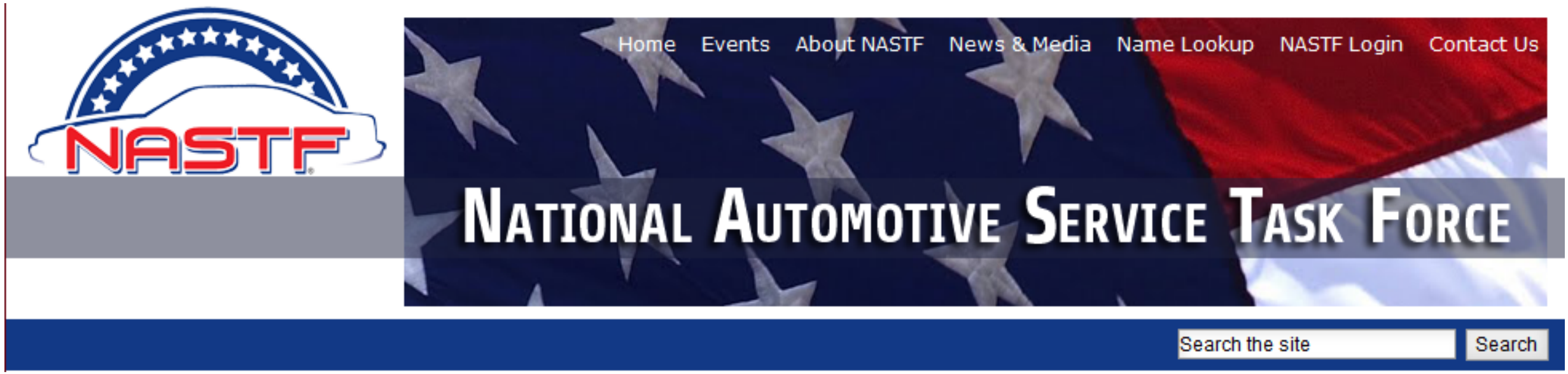
- 6.7.3 Control Vehicle Maintenance Diagnostic Access Diagnostic features should be limited as much as possible to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature. Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they are misused or abused outside of their intended purposes. For example, a diagnostic operation which may disable a vehicle's individual brakes could be restricted to operate only at low speeds. In addition, this diagnostic operation might not disable all brakes at the same time, and/or it might limit the duration of such diagnostic control action.

National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333).

8. Aftermarket Devices. The automotive industry should consider that consumers may bring aftermarket devices (e.g., insurance dongles) and personal equipment (e.g., cell phones) onto cars and connect them with vehicle systems through the interfaces that manufacturers provide (Bluetooth, USB, OBD-II port, etc.). The automotive industry should consider the incremental risks that could be presented by these devices and provide reasonable protections. Aftermarket device manufacturers should consider that their devices are interfaced with cyber-physical systems and they could impact safety-of-life. Even though the primary purpose of the system may not be safety-related (e.g., telematics device collecting fleet operational data), if not properly protected, they could be used as proxy to influence the safety-critical system behavior on vehicles. Aftermarket devices could be also brought on to all ages and types of vehicles with varying levels of cybersecurity protections on the vehicle side of the interface. Therefore, these devices should include strong cybersecurity protections on the units since they could impact the safety of vehicles regardless of their intended primary function.

National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333).

9. Serviceability. The automotive industry should also consider the serviceability of vehicle components and systems by individuals and third parties. The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services.


NASTF
Home
Events
About NASTF
News & Media
Name Lookup
NASTF Login
Contact Us
NATIONAL AUTOMOTIVE SERVICE TASK FORCE
Search the site
Search

About NASTF

The National Automotive Service Task Force (NASTF) is a cooperative effort among the automotive service industry, the equipment and tool industry and automobile manufacturers (OEMs) to ensure that automotive service professionals employed outside the OEMs franchise system have the information, training, and tools needed to properly diagnose and repair today's high tech vehicles.

NASTF Vehicle Security Professional (VSP) Registry Main Page

What is the VSP Registry?

The NASTF Vehicle Security Professional (VSP) Registry is a service created from the NASTF Secure Data Release Model (SDRM), a project of the NASTF Vehicle Security Committee. SDRM is a data exchange system (see graphic below) conceived and designed cooperatively by automakers, the independent repair, insurance and law enforcement communities; it allows the aftermarket to access security sensitive information related to automobiles, i.e. key codes, PIN numbers, immobilizer reset information, and similar types of information. The NASTF VSP Registry program allows access to security-related information while protecting the safety and security of consumers and the integrity of automobile security systems.

Who should use the NASTF VSP Registry and why?

USA-resident* locksmiths and automotive technicians qualified in vehicle security system repairs need a subscription to the NASTF VSP Registry in order to purchase security codes and VIN-specific computer files directly from the OEM/automaker. Most automakers/OEMs make this information available instantly from their websites 24/7/365. See a list of the OEMs and the model year ranges available in **this pdf file (click HERE)**.

Canadian resident locksmiths and automotive technicians can participate in the VSP.

Visit the NASTF Security Registry (SDRM 2.0) sdrm.nastf.org when you are ready to migrating an existing VSC, apply for a new account or add an additional VSC or sub account. Click HERE.

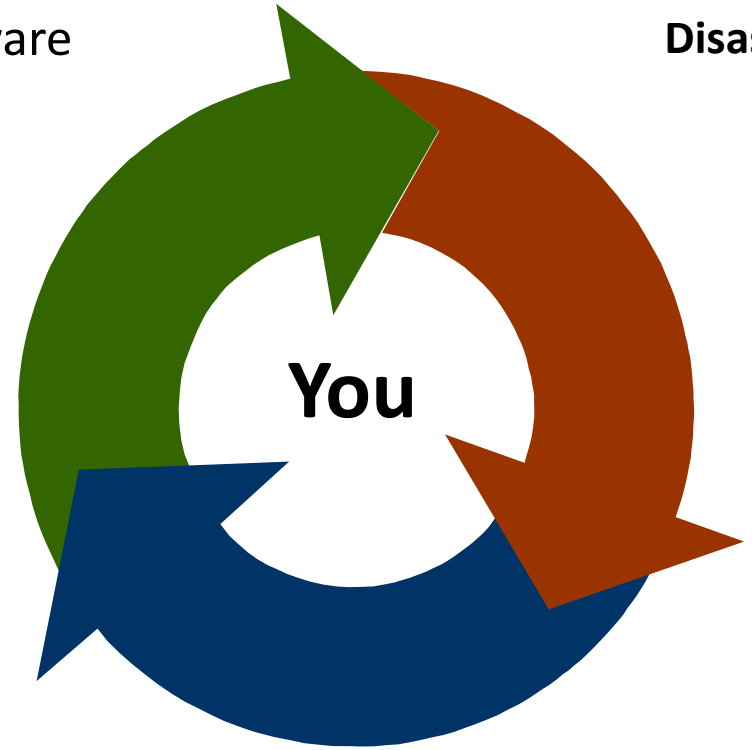
What should you do to secure your shop network?

Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

Prevention, Protection, Security and Recovery

Security

- Anti-Virus / Anti-Spyware
- Patch management
- Firewall
- Biometrics
- Password Protection
- 2 pass authentication
- Encryption
- Spam Filter



Disaster Recovery

- Automated Device backup – 3 Locations

Continuous Education

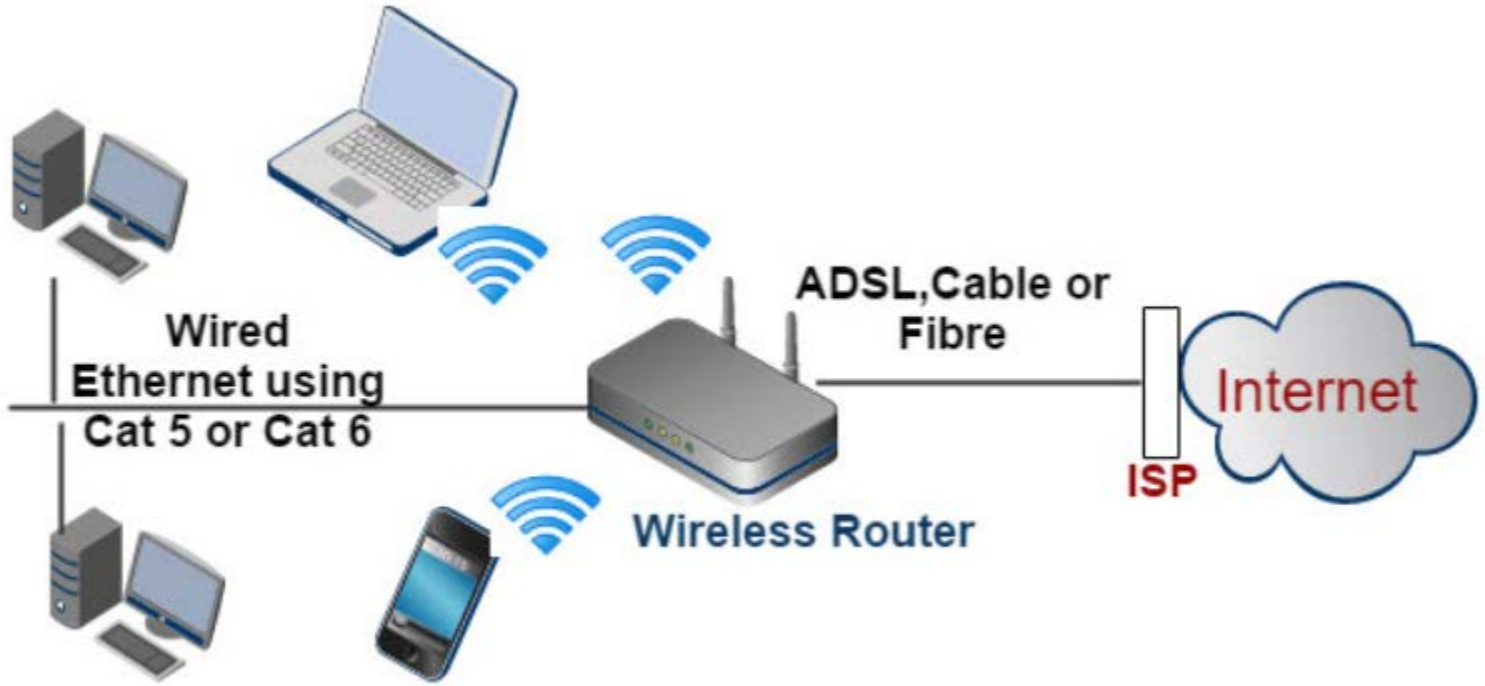
- Best Practices
- Assess and Review

ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

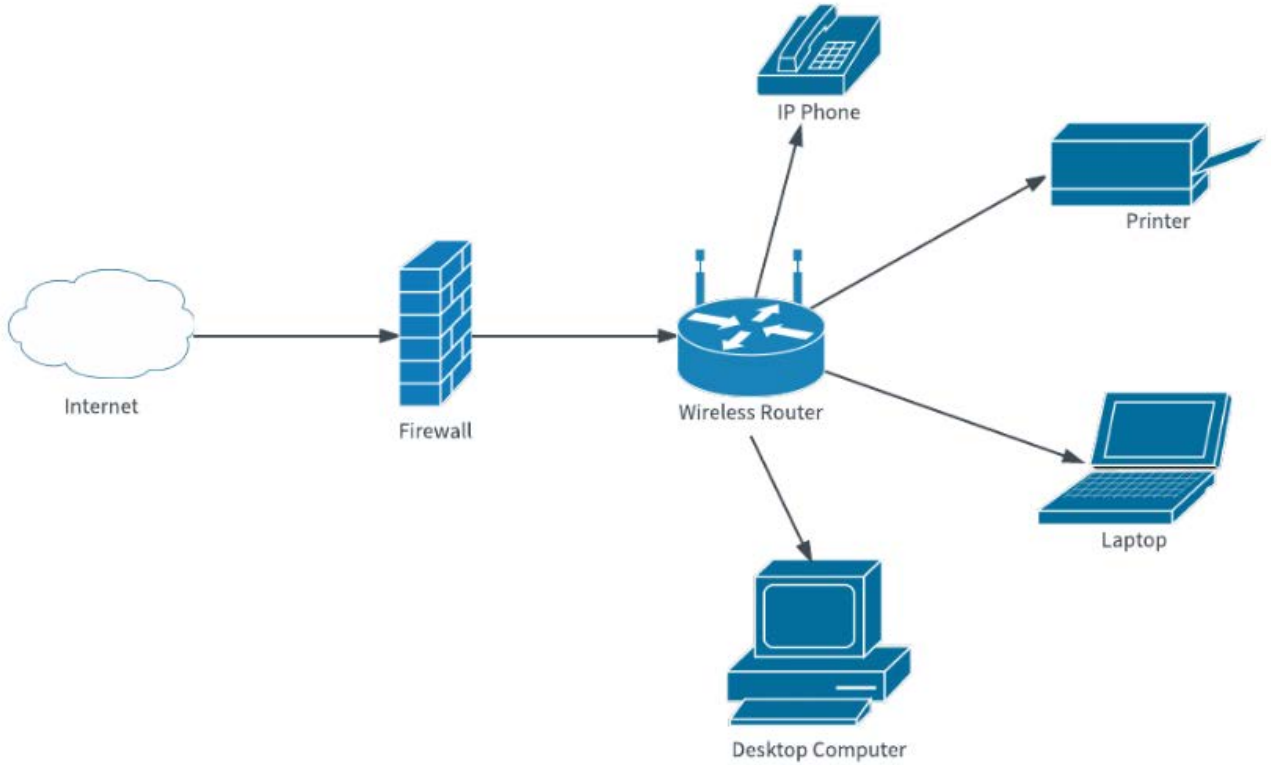
TeamLogicIT
Computer Services. Network Solutions.

Shop Networks

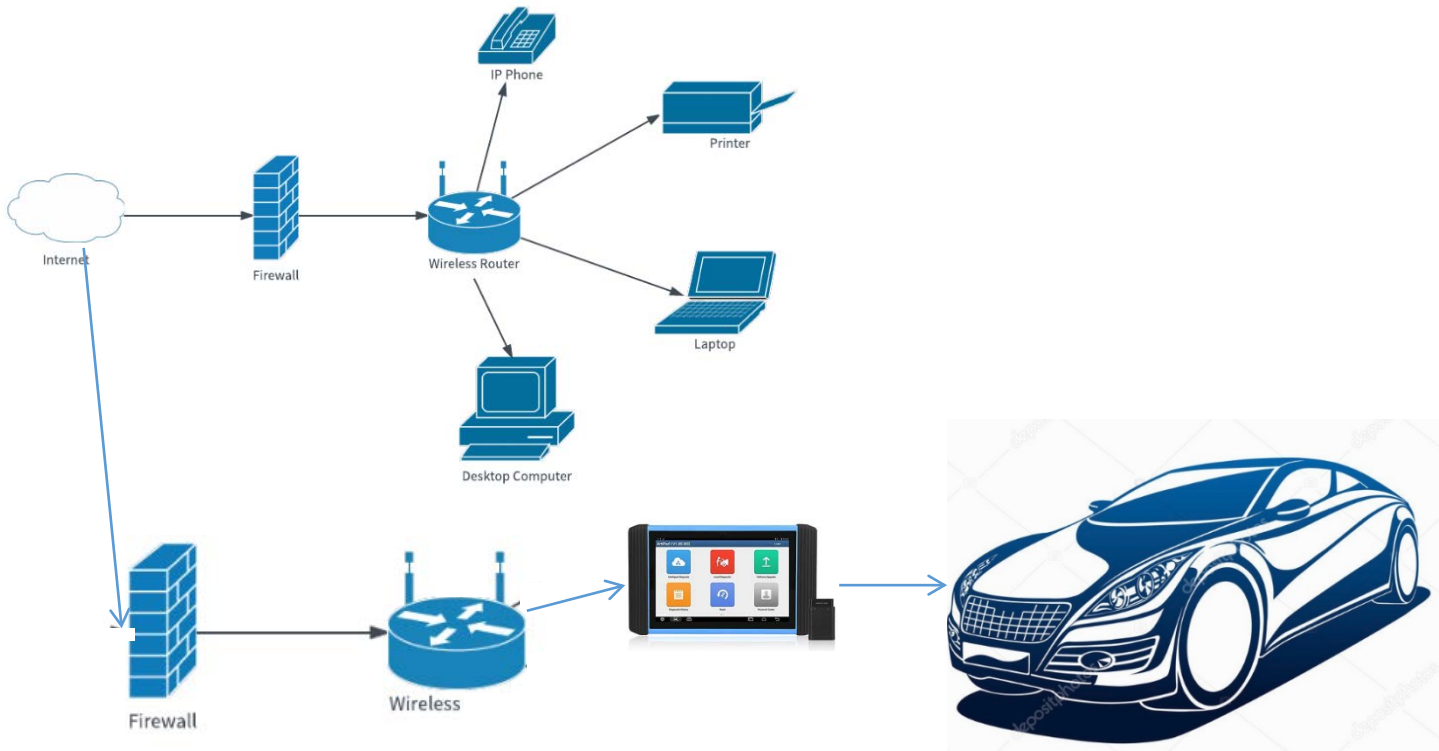
Basic Network Structure



Business Network with firewall



Multiple Networks with Firewalls



Reduce the risks

- Assess the Current Environment
  - What are the technologies that are protecting your network?
  - This is not a one and done activity.
- Address System Vulnerabilities
  - Install patches and updates
  - Ensure backup and disaster recovery solutions are fully operational
  - Develop improvement plans: set investment priorities, schedules, and budgets
- Focus on the “People Problem” Humans are the wild card when it comes to cybersecurity behavior.
  - Create and strengthen security policies
  - Implement awareness training
  - Watch for Anomalies
- Monitor and Validate
  - “checks and balances” help companies ensure their security investments are effective and reduce risk

ASCCA

Automotive Service Councils of California

Professionals in Automotive Service ~ Since 1940

www.ascca.com

Projected cost of the project

Pricing - One time project work

Computer cleanup Labor only

Updates, Registry cleanup, drive space, Anti-virus/malware $150 per station

Server cleanup Labor Only

Updates, Registry cleanup, drive space, Anti-virus/malware $250 per server

Firewall costs per unit

Hardware - Ubiquiti Security Gateway $145

Labor - Configuration and Installation $150

Wireless Access Point with Guest network $149

Configuration and Installation $150

New Computer setup

Windows updates, Data transfer, etc $150

Additional costs for installation of software TBD

My shop with three workstations and no server would be about $1100.00

ASCCA

Automotive Service Councils of California

Professionals in Automotive Service ~ Since 1940

www.ascca.com

TeamLogicIT®

Questions?


ASCCA
Automotive Service Councils of California
Professionals in Automotive Service ~ Since 1940
www.ascca.com

Thank you Walter Edmonson!

TeamLogic IT
408-559-8548
wedmondson@teamlogicit.com