**Delmar Hussey, VCIO at Lifeline Computer Solutions**

His job is to understand their clients' businesses; understand what they do and how they make money. Then he works with them to create a business strategy that helps complement that goal; ensuring that they have the right tools in place. He essentially becomes a consultant for their clients.

Pete Pulido ("Oz"), Senior Engineer Project Manager, designs the systems, puts everything together, and then passes the design off to Delmar for pricing. The team works together to produce the proper system and Delmar remains the point of contact for the client.

Today's talk is about what Lifeline does. When they onboard a client, they start with the Security Breakdown Checklist (slide #2 on page 1). They run a process called Network Detective to identify types of vulnerability:

- What do you have to lose and how important is the loss, timewise?
- Attacks are not pointed but more general; what can the hacker get easily?
- Sensitivity is not a criteria for ransomware hackers.
- Haven't had a problem before...keep it that way.

User Behavior – Vulnerability
Social Engineering Examples include Phishing, asking for permissions/passwords, and fake downloads or attachments. Solutions include: user awareness training and clear company policies that define procedures for suspicious behavior or requests.

A newer example is Vishing; using voice solicitation to extract information or data points that can be used in a later attack. Watch the video here. [This is amazing!] They spoofed the phone store using an app from the App Store that permits you to call someone from anybody's number and hacks a major phone company in only a couple of minutes. How to defend against this type of attack? User Awareness Training.

One audience member shared a story about security, related to a personnel issue. They went into a bank that had recently taken over another bank, and asked for new ATM Cards for both account holders. The account holder provided all the necessary information, verbally, and were issued two ATM Cards that day that would be activated the next day. Absolutely no verification was requested; no ID, nothing with a photo or a signature. This was a major bank, and the person who issued the cards was the branch manager. Stunning!

User Behavior – Best Practices
When accessing sensitive information, always use a secured PC and Network. This includes accessing sensitive company information via a Starbucks Network or other open-access network in an airport of hotel.

Malware can live on anything (phones, USB Drives, MP3 Players), and be designed to run when being plugged-in to even dissimilar hardware. You may inadvertently download malware onto your iPhone and then, when you plug your iPhone into your computer to charge it, that malware can deploy and run the minute it is plugged-in. Solution: charge your phone directly from a wall plug, not via your computer.

Physical Vulnerabilities include passwords, client records, and internal resources. Solution: restrict access to server locations, restrict network access, and lock/shred sensitive information.

Bad file design can also make it easier to grab sensitive information when simply looking at innocuous information. Don't put everything in one table. Isolate sensitive or confidential information.  Suggestion: Make the decision from an educated location; take the time to review legacy systems that have grown organically over time.

Technical Vulnerability
Technical risk examples include: undefined user permissions, weak passwords, screens left logged-in. Solution: Employ best practices for user access/permissions to resources; timeout/lockout policies; security updates, firmware, patches; encryption; password policies.

Network Vulnerability: How do hackers get into your network?

- Port scanning on firewall
- Brute-Force
- DDoS Attacks

Solutions include: Firewall security, network redundancy, current backups and rational password policies.

Also: Hiring an MSP with a large staff that brings a breadth of expertise to focus on a specific vulnerability; have them assess your network's vulnerabilities.

User Awareness – Passwords
This segment of the talk focused on how easy it is to crack passwords and offered suggestions for better passwords. Some really bad—and common—examples, sourced from symatec.com, include (Top Ten):

1. 123456
2. password (4.7% of users use this password!)
3. 12345678
4. 1234
5. pu***
6. 12345
7. dragon
8. qwerty
9. 696969
10. mustang

See the first slide on page 3 for a complete list ... and then change your password!

Break-even point for number of characters is: 8; including numbers, upper and lower case characters, and special characters. A password like this takes a little over two centuries to hack.

Delmar described a Dictionary Attack, where the hacker may use a 5GB file of common passwords (300 miles high of paper), and try all combinations; takes merely hours.
If 91% of people have passwords in the top 1,000 most-common passwords, that means the hacker can get into 91% of systems in less than a minute.

Solution: Make a Password Phrase and substitute some uppercase characters and special characters for letters.
Email Vulnerability
Spam is more than an annoyance; it carries phishing attacks and malware.
Solution: User awareness training; Email security server; Antivirus; and Firewall rules that allow/block specific traffic.

Types of malware that comes into your system via email include: ransomeware; spyware; viruses; worms and Trojan Horses.
Solution: User awareness training, antivirus software, and maintaining current, audited backups.
Statistics are presented on slide 3 of page 5 of the .pdf, and point out that, prior to ransomware attacks, 4 out of 5 businesses believe their backups could provide a complete recovery; after being attacked, only 42% have been successful.

Applications by which ransomware entered the organization include: email link (31%); email attachment (28%); web site or web application other than email or social media (24%); social media (4%); USB stick (3%); business application (1%); unknown (9%).

Email SPAM Statistics indicate that 40% of SPAM email had ransomware (2016), according to IBM.

Defenses against email SPAM are cited on pages 7 & 8 of the .pdf.

Increased Security Options offered by Lifeline Computer Solutions include:

- Email Encryption
- Multi-Factor Authentication (LastPass was recommended; a subscription service) that manages your passwords.
- HIPAA Security User Training Certification
- PCI Security User Training Certification

Contact Delmar via the Lifeline Computer Solutions website.