IT-Support & Planning

Continuance of Operations
December 3, 2014
Let's Get Started

- Introduction
- Presenter(s)
- Company Overview
- NJAMHAA Member
FEATURE FILMS ARE THE RESULT OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF YEARS
Results

• How many found 3, 4, 5, 6 or more?
• Answer is 6! (Word “of” sounds like a “V” not “F”)
• Why couldn’t all of you see all 6 F’s
• Perception!
Technology Assessment

• If you fail to plan, you plan to fail!
• Clear, objective deliverable that identifies risks & vulnerabilities, offering recommendations that are properly identified as High, Medium or Low action-items...easy for management to read
• Picture of where you are today, where you should be tomorrow and a practical action-plan to get you there that follows step-by-step phases
• Nonprofit technology lease options that provide easy, manageable monthly costs for a total refresh/upgrade
Modernize your IT...

- Traditional Premise-Based Build-Out
- Cloud-Based Services
-FileSync Model
Premise Based

• Most if not all of your gear is in your building
• Staffed In-house or blended with an outside organization for support
• Requires a periodic refresh ~ every 3 years which is a capital expense
• Requires management of software licensing with on-going investment as changes occur
• Nominal redundancy for a disaster or business continuity
Cloud

The next stage in the internet’s evolution. The cloud provides the means through which everything (computing power to infrastructure to applications, business processes and collaboration) is delivered as a service to an end user whenever they need it.
Why consider the Cloud?

- **Little to no upfront costs**: Cloud computing users can avoid capital expenditure (CapEx) on hardware, software, and services when they pay a provider only for what they use. Consumption is usually billed like a utility (for example, resources consumed, like electricity) or subscription (for example an annual subscription to a newspaper) basis with little or no upfront cost.

- **Simplified IT support**: many applications available in the cloud require much less in-house IT support because the hosting provider takes care of installs, upgrades, backups and standard maintenance for you.
Why consider the Cloud?

• **No servers** need to be researched, purchased, maintained, or recycled.

• **Rapid deployment:** Often, accounts can be set up in minutes including CRM, accounting and donor management software.

• **Convenience:** Staff and volunteers can access your applications from almost any Internet connection with their login information. No more setting up VPNs or systems to allow remote access to your servers.
• **Loss of connectivity** means loss of access to your software, infrastructure, and data. Also, if you have a slow or unreliable connection, cloud computing isn't right for your mission-critical needs.

• **Service levels**: Make sure that the provider is reputable and provides an acceptable level of uptime and rapid response to issues.

• **Regulatory Compliance**: If you need to be HIPAA- or PCI-compliant or conform to other regulations, make sure your service provider is certified.
Small to medium-sized organizations who have limited capital, limited space, and limited technical staff can benefit financially and environmentally from using cloud computing. It saves energy, reduces the amount of hardware needed, and is often technically easier to install and maintain than in-house designs.
FileSync

File Access from Anywhere...keep all of your data, whether it is presentations, spreadsheets, pictures, or other important files with you wherever you go. Freedom to work from smart phones, tablets, desktops, the web and laptops. Anytime a file is updated, be assured, it will be updated across all of your devices for universal file access.
Quick Riddle

I’m lighter than a feather, yet no one can hold me for very long. What am I?

-Your Breath
Hosted Exchange

• Unlimited Mailbox Storage...no user quotas.
• Performance Optimization...faster, more reliable mobile email.
• Spam and Virus Protection...protect inbound and outbound messages, eliminating up to 99% of unwanted email for every client.
• Mobile Device Synchronization...wireless e-mail synchronization offers users instant access to e-mail, contacts, tasks and shared calendars; increasing business productivity by keeping the workforce connected.
Continuous-Data-Protection (CDP) eliminates premise-based data backup solutions (no more tapes, backup software or human-capital to manage the process)

Local appliance stores data and also streams incremental changes (every 15 minutes) to secure, offsite locations

In the event of server failure, the BDR appliance acts as a standby server allowing for a seamless cut-over while your primary production server is repaired or replaced

Bare-Metal-Restore...drop a complete image of your server (system-state and data) onto the new server...save hours of rebuild time
• Quick show of hands who has premise-based tape backups?
• Who is already enrolled in an online, offsite streaming data backup service?
• Not all CDP services are built the same...who has heard of Carbonite and/or Mozy?
• Client case-study of seamless fail-over
Managed Services

• **Managed Service**...is a web-based technology that monitors the critical health status of devices and applications, remotely diagnosing problems before they occur.

• Notification is delivered through multiple communication outlets in the event of failed network elements such as switches, servers, firewalls along with other critical devices and applications.
Risk Management
- HIPAA Compliance

HIPAA requires entities to protect the privacy and security of both hard copy and electronic Protected Health Information (ePHI). There are general *Administrative* requirements under HIPAA as well as the *Privacy Rule* and the *Security Rule*. The Security rule requires a security gap analysis and risk assessment.
• Vulnerability Assessment (VA) – process of identifying, quantifying and prioritizing the vulnerabilities in a system
• Penetration Testing (PenTest) – simulating an actual attack. May not identify all vulnerabilities.
• Difference is in the scope – is exploitation allowed; how far can you go?
Terminology

- **Vulnerability** – a flaw or weakness in the system security procedures, design, implementation or internal controls that may be exploited
- **Threat** – any potential danger to information or an information system
- **Attack** – an effort by a threat agent to launch a threat by exploiting a vulnerability
- **Risk** – comprised of the factors of threats, vulnerabilities and current value of assets and operational procedures
~ Workstation / Device Security
  ▪ Transfer, removal, disposal / re-use of electronic media

~ Technical Safeguards...
  ▪ Access Control... who can see what?
  ▪ Audit Controls... chain-of-custody access on any given IT-Asset.
  ▪ Integrity Controls... reviewing & refining read-write-execute permissions through Access-Control-Lists (ACL)
  ▪ Transmission Security... moving e-PHI and properly defined security schemes.
Cyber-Liability Coverage

“It can make the difference between staying in business or shutting your doors after an attack”...Inc.

• It’s more affordable than you think
• It can cover more than you think
• You probably don’t have a Risk-Management Team
• Even if you don’t host your data yourself, you’re still responsible
• Your general policy won’t cover you
Case Study

A prospective client requested that Mercadien perform a comprehensive network security and penetration testing. The organization requested that Mercadien test both internal and external vulnerabilities to their network and systems including perform externally based intrusion testing. Starting with only knowing the client name, Mercadien engineers were able to perform a web search to find the company website. That site had multiple email addresses listed in the contact information. Using that domain name as a starting point, Mercadien was able to perform an MX record lookup and a WHOIS lookup to get mail server information and registrar owner information, which was not marked as private. This allowed engineers to not only find the client network IP address but also the email address scheme. Since email aliases are often the same as local user logins, technicians could reasonably assume that accounts existed on the domain with those names.
Mercadien then had an IP address as a target. Since IPs are assigned in blocks, testing was expanded to the (10) IP addresses above and below the target IP. In order to avoid detection, technicians used a MAC address changer (available for free download) and utilized a web proxy to make it appear that the probes were originating from Poland. This was verified after the test as the firewall logs showed all traffic originating from the proxy location. Using a simple online port scanning system, scanning for only common ports, the engineers were able to determine that ports 80 (http) and 3389 (remote desktop) were open to the internet. Port 80 was in fact being used for webmail, and was not secured via SSL cert using https protocols. This was in itself a highly problematic configuration and prone to several methods of attack, however the technicians focused on the open remote desktop port for this test.
Case Study

By launching the default remote desktop application the technicians were able to not only get a response from a server but also see the Windows login screen associated with remote desktop connections. Several free tools exist to perform what is called a "brute force dictionary attack". These tools utilize a dictionary file with over 100,000 common passwords and spelling variations (example Good and g00d). These programs are fully automated and setup to pause for 20+ seconds every 3-4 failed attempts to avoid the user login from being locked due to failed login attempts. Both the "Administrator" account, the account that showed in the registrars domain as the account owner, and multiple other users that were simply common login names (example: ASMITH) were accessed in under 4 hours each.
At this stage, Mercadien was now able to login as multiple users, some of which were no longer with the company and never disabled. Most importantly, the technicians were able to access the domain administrator account which granted them full access to the network. Having server access allowed Mercadien to find the domain controller by finding the servers providing DNS information. Having full domain administrator access allowed them to access those servers, which control all login and security privileges on the network. At this point Mercadien had full access of all servers, security, files and programs on the system.
After the intrusion tests were performed, additional internet vulnerability scans were run. Multiple systems were found to have missing critical security patches, antivirus definitions and weak / missing or default passwords. Out of date patches, antivirus and weak passwords all greatly increase the security risk of not only the system but the network as a whole. Keeping these critical components up to date is one of the most overlooked, yet most simple and effective method of keeping networks secured. Additionally, multiple users who had left the company, still had enabled accounts in Active Directory. This allowed for multiple avenues of unauthorized access.