From: Johnson, Craig (WSP)
To: Trowbridge, Keith; Allen, Erik; Winsor, Debra; Larm, Doug; Evans, Bill (WSFC)
Subject: FW: WSFC status report
Date: Friday, March 20, 2015 9:56:52 AM

One more bit of info.

From: Jarmon, Scott (WSP)
Sent: Thursday, March 19, 2015 7:09 AM
To: Johnson, Craig (WSP)
Subject: FW: WSFC status report

Craig,

The below email is from Andy Amendala. He is one of the two ITD staff that responded to rescue the WSFC during the recent server crash. He had several additional recommendations that the WSFC should seriously consider. Both Bill and Andy did an outstanding job and spent significant time recovering the situation at the WSFC. This comes at a time when they are both stretched very thin with many extremely high profile and demanding projects are underway for the WSP and ITD specifically. Please let me know if you need any additional information.

Thanks,

Scott Jarmon
WSP - MOP Program Manager
Office: 360-596-4921 |Cell: 360-688-0902 | VoIP: 13921

From: Amendala, Andy (WSP)
Sent: Wednesday, March 18, 2015 3:53 PM
To: Jarmon, Scott (WSP); Harwell, Bill (WSP)
Subject: RE: WSFC status report

Your document captured the overall state of the physical servers just fine. A number of items should be included for future failure prevention and better care of their environment. I've summarized them in bullet form here. This list is in no particular order and is certainly not comprehensive.

What the Fusion Center is running is an enterprise IT infrastructure, albeit a small one. Even though far smaller, many of the care and feeding processes and therefore the skillsets, applications, and hardware required are identical to larger environments (like WSP).

- Recruit at least one, preferably two, full-time IT server and workstation support staff. Staff should have extensive experience with the Windows client-server ecosystem and its supporting components – with heavy emphasis on Active Directory Domain Services, DNS, DHCP, authentication, and package/operating system deployment.

  Any viable candidates with a skillset that covers the above will either already have or be able to rapidly acquire any additional skills necessary to be a successful admin in an environment of the Fusion Center's scale.

  Do not compromise on who you hire for this job. If they don't meet the requirements,

they don't meet the requirements. Technical skills in this position are extremely important and are developed over many years of work, not in a span of only months.

- Implement an event monitoring system such as ***HP Systems Insight Manager*** or ***SolarWinds*** to capture hardware and software failure events in a rapid, automated, and centralized fashion. A system like this would catch a hard-drive failure within minutes and send an E-mail to the appropriate staff. At the very least, purchase a lower-end event collection system such as ***EventLog Analyzer*** to facilitate central viewing of logs which while a manual data-mining process, if done regularly (daily), will provide rapid visibility of failure.

- Purchase licenses for a remote support system that can be used by IT administrators without the need to interact with on-site staff (e.g. LogMeIn Professional).

- Thoroughly document the existing and future/intended configurations of the environment in the form of hardware rack elevations, virtual machine locations, and physical network connectivity sheets. This does not need to be complicated. Simple Visio diagrams and spreadsheets would suffice.

- Provide IT support staff the latitude to develop, and with management approval, to implement policy regarding IT behavior and function. During my short visit to the Fusion Center, I witnessed significant violations of even the most basic IT-security practices. (e.g. sharing and storing passwords via written document, unencrypted drives laying exposed, peers changing one another's passwords and using their accounts, etc.) The physical security or classification of the building means very little in terms of the security of its IT architecture.

- Purchase HP Care Pack hardware coverage for all physical servers for their intended lifespan. This will cover all hardware components and in the case of failure, ensure an OEM-replacement part is on site within 1 day at the most.

- Where feasible financially and sensible operationally, purchase Microsoft software products with the Software Assurance (SA) option. This allows administrators the flexibility to obtain bits and upgrade software applications as necessary without waiting for a purchase process or additional funding. Running on the bleeding-edge of technology certainly isn't required, however, the Fusion Center is running far behind on operating systems and application versions – some of which are well out of support. SA would remediate this problem and allow administrators to upgrade at will.

  Running software that is beyond its support window exposes any enterprise to unnecessary security and operational risks.

- Implement a centralized virtual machine management system such as System Center Virtual Machine Manager. This product is often <u>free</u> for enterprises that purchase Microsoft software with SA and is phenomenally useful for efficient, centralized management of virtual machines, regardless of the number being managed. This product's presence alone would have saved over 30 hours of work in the most recent disaster recovery situation.

There's a whole lot more but this is a very good start.

Andy Amendala
Washington State Patrol
360.596.4942

From: Jarmon, Scott (WSP)
Sent: Friday, March 06, 2015 3:04 PM
To: Amendala, Andy (WSP); Harwell, Bill (WSP)
Subject: WSFC status report

Andy/Bill,

Sergeant Johnson asked me for a short summary of the issues with the serves and maintenance at the WSFC. I have created a draft version at this point and would like to ASK you to spend a very little time to provide any correction or details you think need to be added. They are looking for a very basic non-technical document to illustrate what should have been done and/or will need to be done to prevent this from happening in the future.

If you can provide your suggestions, I can format and edit as needed before sending it up.

Thanks again for all you have done for me and the WSFC,

Scott Jarmon
Washington State Patrol
Mobile Office Platform Program Manager
Office: 360-596-4921 | Cell: 360-688-0902 | VoIP: 13921