Thomas Robinson

Unit 12 & 13, Assignment 1

Technical Support

Solihull College
January 2023

Task One U12 P1

Techniques for Support, Troubleshooting & Repair

Software Diagnostic Tools

Software diagnostic tools applications used to test and diagnose problems with a system. There are many types of software that can be used for this: for example, software such as AIDA64 can show hardware telemetry, such as temperatures and fan speeds, as well as running stress tests and benchmarks to verify system performance and stability. Other software used for diagnosing issues include the Windows Event viewer for OS and service logs, the Sysinternals suite for monitoring and antivirus software to ensure a device is free of malicious software.

Remote Diagnostics

Remote diagnostics is the process of diagnosing problems with a computer or computer system while not physically present. TeamViewer is an example of software used for remote diagnosis, where a small client program is downloaded, which a technician then uses to control the desktop remotely.

Fault Records & Logs

Fault records are kept by many physical systems and software logs are commonplace amongst computer programs and applications. These allow a technician to examine the events that took place during an incident, or to spot trends and anomalies in the system’s operation.

Solutions Database

A solutions database contains instructional documentation for solving IT tasks. This could range from everyday occurrences, such as password resets to more obscure technical documentation. These resources are useful for training and as a reference for future incidents. They may also contain specific methods and protocols a company’s IT department may have to adhere to.

Hardware Test Instruments

Testing the hardware of a system or device is just as important as testing the software. There are variety of tools available for testing different

aspects of a system. An example would be a multimeter; this device is used to check continuity, voltage and other aspects of electrical components to confirm they are performing as expected and connected to the correct parts of a circuit board.

Self-Test Routines

Self-Test routines are diagnostic tasks performed automatically or autonomously by a computer. Most computers undergo a Power on Self-Test ('POST') process before the operating system is loaded. This will check the installation of certain components, such as the computer's RAM and CPU, as well as verifying software integrity of firmware and the motherboard's BIOS or UEFI. This can slow down the overall time taken to start a computer, and one has the option of skipping or toning-down the thoroughness of this process.

Specialist Toolbox

Specialist devices are available for many specific tasks an IT technician may need to undertake. An example would be an ethernet cable tester; this can be used by a network technician to verify the connectivity of an ethernet cable and what speeds it is able to transmit and what PoE power it may be able to supply.

Task Two U12 M2

Outsourcing

In-House

Providing technical support in-house is common amongst larger companies with individualised IT needs and operations. The benefits to this method include having named members of a team to build rapport with, and the option of speaking to a human being in-person. Having an in-house technical support also ensures that workers become knowledgeable and acquainted with the company's way of working, their products and their methodology.

The downsides of having an in-house technical support team are primarily cost related. The expense of hiring, and potentially training, new skilled employee(s) may be outside the budget of a smaller company.

Outsourcing

Any level of outsourcing results in a company renouncing some amount of control and responsibility for providing support. There is a risk that the quality of support provided is not adequate.

A significant benefit of outsourcing in general is cost and ease. It is much easier to pay a set amount for a specified amount of service and support when compared to hiring in-house staff.

Local

It is common for companies to outsource IT operations to a local company. This absolves the business of the responsibility of

Remote

Remote support from a foreign country is an attractive option for many businesses. In other areas, particularly emerging markets such as India and Pakistan, provide significantly cheaper options than hiring local talent.

While this is a cheaper option, there are many downsides:

- Support workers will be unable to assist with physical problems, only able to guide them through troubleshooting steps. Lead times on physical issues may be untenable.

- Remote support may not available if there is a technical issue preventing contact with the outsourced company, however an SLA may have provisions to safeguard against this.
- Being from another country, many workers may not have a perfect understanding of English, hampering communication effectiveness.

Mixed

A mixed solution offers an interesting balance of the benefits and drawbacks of outsourced and in-house IT.

A business may choose to outsource lower levels of support to outside companies, however, hire a small team of in-house technicians to respond to physical problems and build a rapport with staff. This provides a middle-ground between cost of hiring and training employees and the many drawbacks of outsourcing.

A mixed solution, however, adds a level of complexity. There may be disagreements between who has responsibility for what. From a users' perspective, having two teams may prove confusing and unnecessary.

Task Three U12 D1

Advances in Systems Support Technology

A significant development in IT system support—and support services in general—is the implementation of virtual agents and chatbots. In some instances, these make use of AI, however most are just implementations of a process tree.

A prominent example of this is Vodafone's TOBi. This is marketed[1] as a 'digital assistant' that can perform many tasks that previously required a human at the other end of the conversation. There are several benefits and drawbacks to chatbots such as this.

Providing 24/7 help is a prominent benefit to a virtual agent. There is no need to keep members of a support team on-call through the night to answer simple, routine queries. Customers are able to work through basic problems with the virtual agent whenever is convenient for them.

Virtual agents can also act as a directory to human workers and knowledgebase articles. This is another benefit touted by Vodafone's TOBi. If the chatbot is unable to resolve a query, then it can intelligently assign a knowledgeable human to step-in and provide assistance. If a support article exists on a related topic, this can also be presented to the customer.

Vodafone leans heavily into marketing their chatbot and its merits, while some companies obscure the fact that one is not talking to a human. This is one of the most significant hinderances that plague many chatbots. This can provoke frustration when inadequate support is received, or the bot is unable to understand an issue.

Limited functionality is another issue that can be found within the space of digital agents and chatbots. If the bot is only able to search a knowledgebase and provide links to articles, a user may consider why the chatbot exists in the first place when it could be replaced with a clear search bar. This ties in with the lack of transparency; a user may feel especially deceived if they expected to receive support from a human and instead were directed to documentation or an article that can only provide general guidance.

[1] https://www.vodafone.co.uk/contact-us/

Task Four Part One U12 P1

Impacts on Technical Support Provision

Organisational Guidelines

Organisational guidelines affect the provision of technical support primarily by regulating certain aspects of operation. This includes the reporting of faults. For example, an organisation may mandate that any fault that is found while undertaking technical support is logged. The process of logging a fault may be seen as overzealous and slow down the task of troubleshooting and repair. Other potential guidelines include the use of the internet. It may arise that a site required for researching a topic is unavailable or blocked, making it difficult or impossible to diagnose or fix a problem. Security in an organisation also has an impact on IT support, for example technical support workers coming across sensitive information during the course of their job needs to be acknowledged by the organisation, as well as the unique level of trust placed on them when support is given.

Confidentiality & Sensitivity of Information

Working in an environment that deals with confidential information requires that the technical support team be diligent and trustworthy. As mentioned previously, working with IT resources of employees and of the company requires some level of access to potentially sensitive information.

Costs of Resources Required

The resources required to provide in-house technical support are numerous and come with a cost. At the very least, it is required to have a member of staff knowledgeable about the company and the IT infrastructure in place. Additional quality-of-life tools may be requested, such as monitoring software and a ticketing system. These impact the provision of technical support by adding additional employees and services that need to be managed and looked after, as well as new resources that other employees might need to be trained to make use of.

User Expertise

Training staff is a large part of an organisation’s role in creating a strong workforce. If IT training and basic troubleshooting is included in this

training—or those hired are screened for IT literacy—the number of 'simple' issues being reported to technical support will likely be less than it otherwise might. If a user is able to undertake basic troubleshooting tasks and attempt to solve mundane issues themselves, they are less likely to need to burden a member of technical support. This ensures there is the time available to respond to and deal with higher priority issues.

Outsourcing of Support Services

Outsourcing some or all a technical support team's role is one of the largest decisions that can be made regarding it. A mixed solution, where some tasks are handled by an on-site or in-house team, offers the best of both worlds, though adds significant complexity and comes with its own downsides. Any level of outsourcing risks lowering standards and providing a sub-par service to the organisation, particularly if the third-party is located overseas where the populace may not have a good grasp on the English language.

Task Four Part Two U13 P1

Impacts on Troubleshooting & Repair

Organisational Policies

As with providing technical support, providing troubleshooting and repair services within an organisation can be affected by policy. Security implications, such as confidentiality, may impact the areas or resources that IT can access freely. Organisational costs and budgets may not allocate enough resources to the service, leaving equipment unmaintained. This leads to IT having to prioritise what gets looked at, leaving some tasks—and some users' issues—unresolved, potentially for extended periods.

Contractual Requirements & SLAs

Contractual obligations can dictate the time at which repairs take place and the urgency with which they are dealt. For example, a company may state that some types of issues are fixed within a certain timespan, or that maintenance be carried out in pre-allocated windows of time. Service Level Agreements may dictate the uptime and availability of a service or resource, necessitating backup or failover solutions.

Legislation

Laws and regulations can play a key part in the provision of troubleshooting and repair. The Computer Misuse act, for example, forbids access to systems without prior permission or authorisation. Health and Safety rules touch on proper posture and safe working practices. An organisation dealing with Personally Identifiable Information needs to act around the Data Protection Act and GDPR, while one working with privileged Government Organisations may be privy to information held under the Official Secrets Act for national security.

Internal Issues

Within the organisation, internal issues can plague an IT department, for example, the attitude of employees and general workplace morale. A company with poor rapport with its staff is unlikely to have workers that go beyond, and this includes those undertaking troubleshooting and repair.

Communication with Customers

During issues, it is important that IT are as transparent as possible during the troubleshooting and repair process. This ensures that customers are kept up to date. A popular way of doing this is to provide a status page, showing current resource availability, current and past issues, as well as the option to subscribe to update notifications.

Task Five Part One U13 D1

Impact of Faults

Technical faults-whether it be hardware or software, major or minor—can have a significant impact on the organisation.

Hardware Faults

Hardware faults cover physical equipment failure and mechanical issues. This could be anything from a failed component in a server to a natural disaster destroying equipment. Depending on what is impacted, there can be significant impacts.

An example of a hardware fault would be drives in a server failing. If this server was hosting business-critical data, then it is likely that there will be a loss of data. Unless a constantly synchronising, incremental backup is configured, data created since the last backup may be lost. Likewise if there was no redundancy, in the form of RAID or an alternate server, employees will be unable to continue working until the fault is rectified. This lack of access to resources could cost the business significantly in lost productivity. The financial impact of this lost productivity and lost data may be substantial.

A similar scenario causing disruption would be the failure of a piece of network infrastructure, for example a switch. Depending on where this failure lies—within the company or with the ISP—this may prohibit access to resources required for employees to do their day-to-day duties. This, again, poses a risk to productivity and by extension, costs the business.

Hardware faults are often trickier to diagnose since many devices do not feature screens or speakers for diagnostic output. For example, a basic network switch may not have any method of collecting diagnostic information at all.

Software Faults

Issues with software can affect any organisation.

Bugs and issues with software that cause instability or crashes can be frustrating for staff. Time spent recovering from a crash or working around a bug or unexpected behaviour is lost productivity. Crashes can cause loss of data that was currently being worked on if the program was not designed to handle them.

A fault leading to a security vulnerability can place the organisation at peril. If personally identifiable information is exposed, it can open the organisation up to the wrath of legislation and the consequences that come with improper data handling. In many cases, this is a significant fine or penalty.

Minor Issues

Even the smallest of issues can have a culminative effect on the business. Both hardware and software issues, if frequent, can be 'death by a thousand papercuts' for the business. Examples of minor issues include slow internet or a malfunctioning printer. Not resolving these faults can lead to low morale and poor productivity. There is no significant outage or major event, but business still suffers.

Examples

A well-publicised example of an impactful software fault is Fujitsu's Horizon. This accounting software was introduced across branches by the Post Office in the late 1990s and early 2000s. The system was suspected to be unreliable; often producing accounting errors that led to significant shortfalls between reported revenues and takings. The Post Office wrongfully prosecuted hundreds of postmasters for fraud and false accounting, leading to several convictions, fines and prison sentences. Many postal workers impacted lost their livelihoods, were plunged into significant debts, or were wrongly imprisoned. Tragically, many believed the Post Office and their adamance that it wasn't their fault, with a worker from Cheshire taking his life after a shortfall of thousands of pounds was alleged. Despite the Post Office and Fujitsu's arrogant insistence into the early 2010s, they eventually conceded that the software may have been to blame.
Many—even seemingly minor—faults and failures can lead to very human consequences, and this case only exemplifies why they should be investigated, acted upon, and fixed.

A less impactful example of hardware failure affecting a business is the failure of a storage server at Linus Media Group, a media production company that runs several successful technology-related YouTube channels. A faulty RAID card led to the failure of a storage array. With limited fault logging, it was difficult to diagnose the root cause of the issue. In the end, a remote data recovery company was contacted who were able to successfully reconstruct the data. This whole scenario caused

significant disruption to the company: the server was used to store everything from employee reviews to in-progress video shoots that were not backed up in any other location. The unavailability of the server meant the company was unable to produce videos or conduct day-to-day business operations, and the data recovery had a deep financial penalty.

Task Five Part Two U12 M1

Importance of Fault Logs

Fault logs are a critical tool for identifying and resolving issues. They are records recorded by hardware and software that detail anomalies. A typical fault log entry for a device will include the date, time, circumstances as well as a specific error message or code.

One of the primary purposes of a fault log is to aid in providing detailed information about the nature of a problem. For example, a computer's BIOS may log detected hardware errors within the system and display them to a user, allowing them to take action to rectify the fault. It is typical for software to keep log files, which may contain any errors that occur during their use.

Analysis of fault logs can help an IT team pinpoint the root cause of an issue or fault, which can help them take the appropriate steps to fix it. Often, a detailed fault log can skip many steps of manual troubleshooting. Using the example of a computer system again, the BIOS keeping a log of faults meant there was no need to test each component individually when a fault occurred.

Pre-emptive monitoring of fault logs can be used to identify patterns and trends with devices. A piece of software or a hardware device may not fail all at once, so being proactive in checking the fault logs can allow an IT team to resolve smaller issues before they compound. Further analysis and monitoring can show trends within the organisation, facilitating futureproofing.

Keeping certain fault logs may also be a requirement of meeting compliance legislations. They demonstrate that a business is showing appropriate due diligence and can also demonstrate that systems meet specified Service Level Agreement standards.

In summary, a well-maintained and effective fault log management system can help an organisation identify and resolve technical issues promptly and assist in minimising downtime and lost productivity.