Cybersecurity and the Evolution of the Customer-Centric Service Desk

Maryam Rezaeian, University College London, UK
and
Martin Wynn, School of Business and Technology,
University of Gloucestershire, UK

Email: M.Rezaeian@ ucl.ac.uk
Email: MWynn@glos.ac.uk

***Abstract* – Cybersecurity is now seen as a central function of the modern IT Service Desk. This article examines two case studies of Helpdesk or Service Desk operations in different technology eras, and highlights the recent emergence of Cybersecurity as a critical area of Service Desk responsibilities. The article profiles the Helpdesk operations at Glaxo Pharmaceuticals in the late 1980s and the Service Desk functions at the University of Gloucestershire in 2019. Comparative analysis shows that whilst the range of technologies requiring support has increased markedly, this has been counter-balanced somewhat by the emergence of standards and dominant products in many technology categories. Cybersecurity, however, has emerged as a key concern that permeates all fields of Service Desk support. It also finds that the role of the end-user has evolved significantly in a rapidly changing technology landscape.**

Keywords – Cybersecurity; Service Desk; Helpdesk; customer-centricity; office systems; personal productivity tools; business systems; end-user computing.

I. INTRODUCTION

The advent of the personal computer in the 1980s and the subsequent widespread use of the Internet and mobile technologies ushered in a revolution in corporate computing that has required a step-change in end-user support and Service Desk capabilities [1]. Amongst these new capabilities and competences, Cybersecurity has become a key element of Service Desk support, and its significance to corporate sustainability is only likely to increase in future years. An enterprise security review recently concluded, "Cybersecurity now lies at the very heart of the corporate and public sector agenda" [2] and the complexity and far reaching nature of Cybersecurity is well illustrated by the multiple lawsuits being pursued against Apple Inc. As reported in the Washington Post, FaceTime (Apple's video chat application) "suffered a security glitch that enabled users to 'eavesdrop' on conversations and see individuals through their iPhones without detection" [3]. The bug was fixed only two weeks after its discovery, resulting in concerns around both personal and business security. Another pertinent example surfaced in July 2019, when it was revealed that British Airways faces a £183m fine over a security breach that occurred in 2018 - a record fine for a data breach and the first to be levied under the General Data Protection Regulation (GDPR) in the UK [4].

Back in 1988, there was virtually no use of the Internet, portable computers were in their infancy, there were no mobile phones or tablets, and the issues surrounding Cybersecurity were very different. Although the personal computer (PC) had broken through to become the main desktop device in the more technology advanced organisations, local area networks were just being introduced and MSDOS was the main PC operating system in the pre-Windows age. Many of the mainstream corporate systems were bespoke (often in 3G languages like COBOL), and the main packaged software products like the SAP and Oracle Enterprise Resource Planning (ERP) systems were just starting to be taken up by the bigger corporations.

Support for such technologies is a key issue in nearly all organisations today, and this article examines the origins and evolution of end-user computing and support functions over the past three decades, and focuses specifically on the requirements to ensure effective Cybersecurity. It features two case studies. First, Glaxo Pharmaceuticals, which was an advanced technology user and was seen as a leader in its rapid uptake of PC applications in the 1980s [5]. The second case study concerns the University of Gloucestershire (UoG) in 2019.

This introductory section is followed in Section II by a brief discussion of the background to this research and the case study methodology, and sets two research questions. Sections III and IV discuss the two case studies and section V then focuses on Cybersecurity and suggests an outline checklist for Service Desk monitoring of Cybersecurity issues. Section VI addresses the two research questions. Finally, Section VII summarises the research findings featured in this article.

II. BACKGROUND & RESEARCH METHOD

IT services are key in ensuring the efficiency and agility of business processes, and the importance of a successful Helpdesk or Service Desk in supporting corporate performance is generally accepted. As early as 1992, Bridge and Dearden [6] noted "the quality of Helpdesk operations can be improved by the provision of knowledge to front line Helpdesk operators" and that "this could only be done effectively if AI technology is used". This early study of Helpdesk operations proved prophetic, as Helpdesks have evolved to meet the changing demands of end-users and have used increasingly sophisticated support systems. Existing literature also highlights the increase in the range of technologies that Helpdesks are required to support. Gonzalez, Giachetti and Ramirez [7], for example, note that

the average number of information technologies supported by central support functions has increased from 25 to 2000 in the current millennium. Sood [8] recently noted, "The cross-functional nature of its operation means the help desk directly impacts productivity and is an essential part of what enables an agency to meet its stakeholder needs".

One of these needs is to ensure protection against hackers and outside interference or unauthorized access to an organization's systems and the data they contain. This is normally termed "Cybersecurity" which is defined by the National Institute of Standards and Technology [9] as "the ability to protect or defend the use of Cyberspace from Cyber-attacks". More specifically, the Economic Times [10] see Cybersecurity as "the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation." The main areas covered in Cybersecurity are:

- *Application Security*, which "encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance."
- *Information Security*, which "protects information from unauthorized access to avoid identity theft and to protect privacy."
- *Disaster recovery planning*, which is seen as a process that "includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster."
- *Network security*, which encompasses "activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network" [10].

Effective and robust Cybersecurity requires measures based around "three pillars: people, processes and technology" [11]. This approach can help organisations "defend themselves from both highly organised attacks and common internal threats, such as accidental breaches and human error" [11]. As a Chief Information Security Officer (CISO) recently noted, "by aligning security with the technology function, it is considered a technology problem to fix, but what we know now about security is that it transcends many different frontiers of business, that it's a people, process and technology problem to fix" [2].

People: All members of staff and (in the context of a university) students need to be aware of their role in preventing and reducing Cyber threats, and specialist Cybersecurity technicians must remain abreast of new developments, with new skills and competencies to mitigate and respond to Cyber-attacks.

Processes: Processes are crucial in defining how the organisation's activities, roles and documentation are used to mitigate the risks to the organisation's information. Cyber threats change quickly, so processes need to be continually reviewed to be able to adapt with them.

Technology: By identifying the Cyber risks that an organisation faces, the necessary controls can be put in place. Appropriate technology can be deployed to prevent or reduce the impact of Cyber risks, depending on risk assessment and what is considered an acceptable level of risk [11].

This article looks at two case studies of relevance, spanning a thirty-year time gap. The case study is a widely used methodology within business research and Bryman and Bell [12], for example, argue that the case study is particularly appropriate to be used in combination with a qualitative research method. A case study facilitates detailed and intensive research activity, usually in combination with an inductive approach as regards the relationship between theory and research. Saunders, Lewis and Thornhill [13] argue that case studies are of particular value for explanatory or exploratory investigation.

Data collection was pursued through participant observation and action research. One of the authors worked at the first case study company (Glaxo Pharmaceuticals) as IT Trainer and then End-User Computing manager in the 1984-88 period. Some of the observations included here were discussed in research publications at the time [5] [14], and these have been used as secondary sources of material. The other author has worked on the IT Service Desk at the second organization (UoG) and thus has first-hand experience of the technologies deployed and the Service Desk operations. There are thus multiple sources of evidence, which as Yin [15] suggests, is one way of increasing the construct validity of case studies. At UoG, this includes participant observation and a number of internal reports and policy documents, particularly those concerning Cybersecurity.

Within this context, this article addresses two research questions (RQs):

RQ1. How have the support requirements of Helpdesks and Service Desks evolved over the past thirty years?

RQ2. How has the Service Desk developed in response to the need for Cybersecurity?

III. CASE STUDY 1: GLAXO PHARMACEUTICALS 1988

Overview: In 1985, the European shipment of PC workstations overtook shipments of simple terminals (i.e., video display units and keyboards, with very little processing power), with computer users taking advantage of new word processor, spreadsheet, graphics, email and database applications running on their PCs. Within this change environment, Glaxo Pharmaceuticals saw a rapid increase in the use of PCs, which transformed the nature of computing within the company. In excess of 1300 PCs were installed in the company's four sites at Greenford (London), Barnard Castle (County Durham), Ware (Hertfordshire) and Speke (near Liverpool). This expansion reflected the dramatic growth and improvement in PC-based office systems during this period. However, in 1984, office systems were clearly a function of the HP3000 mini-computers, there being over a thousand users of these office systems in Glaxo, over 600 of which were electronic mail users. There were just a few PC-

based users of spreadsheets in the sales, marketing and market research areas. By 1988, one in four staff had a PC, and of these, six out of ten had a spreadsheet, four out of ten had a graphics package and a word processor, and three out of ten had a database package. The use of mini-computer graphics modelling and word-processing had virtually disappeared, but electronic mail remained a function of the Hewlett Packard mini-computers, there being over 2,500 users, a fourfold expansion since 1984.

Word processing and desktop publishing: In the period 1984-88, word-processing experienced several phases of growth. In the two years after 1984, the company standardized on one main word processing system (HPWord), based on an HP mini-computer for all secretarial/office staff. Then, in 1987-88, as the PC became the standard desktop machine rather than the terminal, users were transferred to a PC-based version (PCWord) of the software, thus minimizing the need for retraining. Then in 1988, the company embarked on a further change that would see the introduction of a more sophisticated word processor as the standard for secretarial use. This was in part driven by the well-publicised benefits of using the so called "desktop publishing" (DTP) packages, which required a skill level normally beyond that of the average secretary, and which also required specialist workstations (an 80386 chip, and a PostScript-compatible printer) if acceptable performance was to be achieved.

TABLE I. END-USER COMPUTINGE SYSTEMS AT GLAXO PHARMACEUTICALS 1988

End-user system name	Software
Electronic faces folder	DB3+/Tencore
Medical records	DataEase
Unpublished journals	DataEase
Label reconciliation	DataEase
Materials requisition	RBase 5000
Medical terms dictionary	Custom-built in PASCAL
Accident records	DataEase
Project engineer management	DataEase
Media scheduling	DataEase
Planning & budgeting	DataEase
Action reporting	DataEase

This resulted in the introduction of only two desktop publishing workstations (running PageMaker and/or Ventura software packages). However, it was expected at the time that the standard document processing software available to secretaries would come to include some DTP functions such as graphics and scanned image importation, and this is indeed what happened. It was thought that a move to the type of mid-range product in the word processing to DTP spectrum (such as the Lotus Manuscript or Advancewrite Plus software packages) would be beneficial. The coming of Windows as the standard operating system and the gradual dominance of the Microsoft Office products was not envisaged at that time.

Databases and spreadsheets Databases are possibly the most powerful end-user tools of all the functional "off- the-shelf" packages, while spreadsheets are the most commonly used. A PC survey carried out at Glaxo in May 1988 found that for every PC database system written by the company's Information Management Division (IMD), end-users had developed three systems for themselves. The PC systems developed by IMD at the request of end-users is shown in Table I. Authorisation for these systems was done on an *ad hoc* basis, and approval for resource allocation from higher management levels was not required. A number of different spreadsheet packages had been tried by end-users, but Lotus 1-2-3 was the most commonly used.

Graphics packages: Graphics packages were not as common as word processors, but the two were increasingly used in unison as standard secretarial software. They were used mainly for departmental reports and presentations. The data was still input manually for the most part, but electronic transfer into graphics packages was on the increase as integration with mainframe databases and other office systems improved. This was to be a forerunner of the wider integration and consolidation of office productivity tools that occurred in the Microsoft era. By 1988, the main graphics package used was Freelance or Freelance Plus, which was then from the provider of the Lotus 1-2-3 spreadsheet, ensuring ease of data transfer between the two packages.

Electronic presentations systems and presentation design software: This was a significant end-user computing activity. There was a range of software packages available for electronic systems, including PictureIt and Freelance Plus, running on the so-called "IBM compatible" PCs. PictureIt enabled the user to design bar, pie, line, organization and word charts in a range of pre-determined formats. It was extremely easy to use and yet contained sufficient variety to facilitate the design of a reasonable presentation. This was particularly useful for senior management and the sales and marketing functions.

For more specialised needs, Freelance Plus was used. This was a freeform drawing package, with a range of icon libraries that could be combined with PictureIt images. Graphs could also be imported from other software packages (including Lotus 1-2-3 and Lotus Symphony). Standard 80 column/25 line text screens could also be converted to VideoShow format and edited using VIP.

The VideoShow presentation system was made available to be taken out on loan from the IMD, and each of the four sites had at least one of these machines. Having prepared the presentation with software running on the PC, this was then saved to "floppy disc" and run on the VideoShow presentation system. These presentations could be given to a large audience via a projector (e.g., Barco Data 3 or Electrohome ECP 2000) or a colour monitor for smaller audiences. The wide range of colours available (1,000) as well as the range of formats available made this a convenient way to present material

suitable for a 35mm slide presentation. The obvious advantages included the portability of the presentation (one floppy disc could hold as many as 200 images) and the fact that the presentation was always in the correct order, the right way round and there were no focusing problems.

Computer based training (CBT) packages: From 1985 onwards, approximately 30 CBT packages were developed by IMD using the Tencore authoring language [16]. Most of these were for sales and marketing training, and their support and on-going enhancement and update constituted an element of PC systems support at the time.

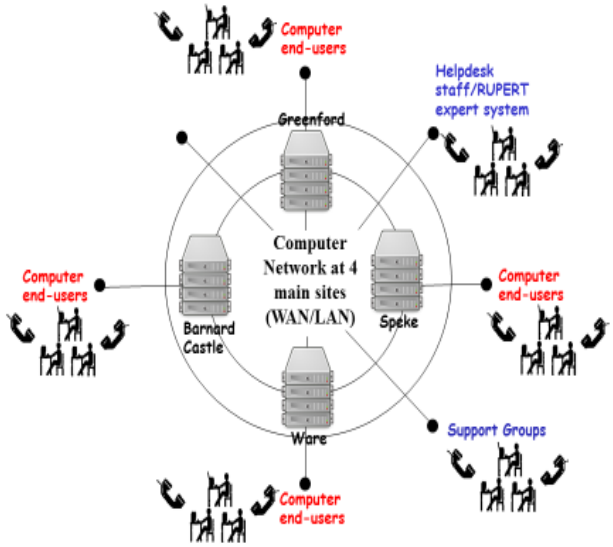

Figure 1. The Rupert Helpdesk system: interaction with end-users and support groups.

The Helpdesk function: The Helpdesk was centralized at the company's Greenford site, but had links to support staff in the company's three main manufacturing plants at Ware, Barnard Castle and Speke (Figure 1). By 1988, IMD had developed its own in-house fault logging diagnostic system, built using an expert system shell (CASSANDRA). This system was known as "Rupert" (Resolves Users' Problems Expertly).

The Helpdesk had hitherto been manned by a senior network analyst who used his expertise to help solve users' problems. Rupert encapsulated some of the experts' knowledge and was able to apply it to users' problems. By asking a series of questions, Rupert could home in on a problem. In some situations, it could take action such as aborting a users' session, disconnecting a terminal or asking the user to perform some action such as pressing a key etc. In other cases, where Rupert was unable to provide a full solution, the call was passed on to the support group, which, in Rupert's judgement, would be best placed to deal with the problem.

The support groups were still in the main geared to helping users of the company's wide range of bespoke transaction processing and reporting systems for their manufacturing and financial functions. These were mainly written in COBOL or PASCAL, and the analyst-programmers of the day doubled up as support staff to help end-users. Indeed, for the main manufacturing system (known as "MENTOR"), there was a programme of courses run on the four sites on test machines on which the main manufacturing systems could be simulated. There were three main support groups for the main corporate business systems and a fourth for office systems and end-user computing. The main business systems were run on Hewlett Packard mini-computers at the four sites linked by a wide area network, and there were a number of test and development machines.

It was in these support groups that security issues of the day were managed and problems resolved. The main concerns were less about Cyber threats from third parties, but rather about human error corrupting data. There were particular requirements in the pharmaceuticals industry in relation to Good Pharmaceutical Manufacturing Practice (GPMP), notably stock traceability in the event of damaged or defective products, and process validation, which required high levels of access control and back-up procedures, above all in the MENTOR suite of programs. The concepts of application and information security, and disaster recovery planning, were in evidence in what was an advanced blue-chip company; and network security was of paramount importance in ensuring the transfer of data and information via the WAN that linked the company's four sites.

More generally, the Rupert Helpdesk system produced fault statistics, which helped IMD to identify problem areas and thus continue to improve the service given to users. The major benefits of Rupert to the company were:

- its role as a training aid for new Helpdesk staff;
- the ease with which new knowledge could be added to the system;
- the time taken to resolve user problems was halved;
- the improved image of IMD in the rest of the company;
- the better statistics it provided about user problems.

The last two benefits could probably have been obtained from any Helpdesk function and fault reporting software. However, Rupert's excellent user interface made this a very successful application of expert system techniques. It was envisaged that the system would eventually be the focal point of a comprehensive network management system.

IV. CASE STUDY 2: UNIVERSITY OF GLOUCESTERSHIRE 2019

Overview: UoG is located across six sites within Cheltenham and Gloucester with 20 professional departments. The Library, Technology and Information Service (LTI) department provides supports for both staff and students, particularly for teaching and learning, along with the provision of appropriate training and skills development. The University has over 1,500 staff, most of which are computer users, and approximately 10,000 students, who use a range of applications on University equipment in labs and classroom environments. The IT Service Desk is located within LTI and provides full support for staff in University hardware, communications and software solutions. Support for students encompasses Office 365, assignment submission, the Moodle

learning management system, and a range of IT guides accessible via MyGlos Help (a web portal guidance page which helps student to search for guidance and information).

TABLE II: MAIN BUSINESS SYSTEMS SUPPORTED BY UOG LTI

System	Description
Sunrise	IT application to manage enquiries from students and staff
SITS Student Records	SITS is a student records management system used to store, administer and manage all aspects of student information from initial enquiry and application through to degree congregation. A configurable package from software provider Tribal.
ResourceLink	ResourceLink is an integrated HR and Payroll software package.
Agresso Finance	A global accounting system from software provider Unit4.
Moodle	Moodle is a free and open-source learning management system written in PHP and distributed under the GNU General Public License.

Office productivity tools and end-user computing: Microsoft Office 2016, Adobe, SSRS, SPSS, and NVivo are the main packages that are increasingly used as standard on a daily basis. SSRS (SQL reporting) is mainly used for departmental reports, whilst SPSS and NVivo are only used for teaching and research purposes, and PowerPoint (part of Office 2016) is the main package used for presentations. There are many different packages on different machines, depending on department needs. For example, there are 150 graphics package users in the Departments of Art and Design and Landscape Architecture. The operating system for the PCs is currently Windows 7, although a University-wide upgrade to Windows 10 is currently being rolled out. The University email system is based on Microsoft Office 365 and hosted externally. The University supports Office apps such as Skype for business, Outlook, OneDrive, and uses the international roaming service called Eduroam to provide Wi-Fi connectivity. Eduroam allows UoG users to login at any participating institution using their UoG login name and password. Eduroam also allows users from any participating institution to login to UoG using their local login name and password. LTI use Gmetrix to provide Microsoft Office training to both staff and students. UoG supports staff and student research projects with SPSS and NVivo.

As regards telephony, the internal telephone system (an Avaya IP phone system providing telephony for all the University campuses and the majority of the student halls of residence) is complemented by a number of exchange lines direct from the BT exchange. These are used for alarm lines, swipe machines for debit and credit cards, and payphones around the University and in halls of residence. LTI are responsible for managing mobile phone services, which are coordinated through a centralised agreement with Vodafone. The University will provide support for equipment and software, which is procured by the University, but does not support mobile phones, tablets or other equipment purchased by staff or students themselves. Nevertheless, the frontline support teams will endeavour to help students with their own devices if they can (e.g., to reinstall software or attempt data recovery), but they will not attempt to fix any major hardware or mechanical problems.

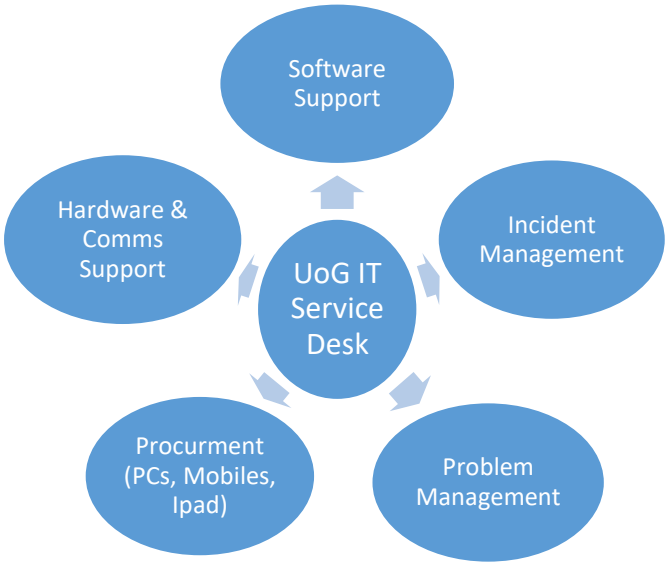

Figure 2. Main operational functions of the UoG IT Service Desk 2019.

UoG Main Business Systems: There are about 60 business systems running across the University, including Sunrise, SITS Student Records, ResourceLink, Agresso Finance and Moodle (Table II). All of these are now supported by LTI, although some started as departmental end-user systems prior to the centralisation of IT support within the University and the imposition of certain policies and standards. Many of these systems are administered by end-users who undertake data maintenance and general support tasks. The SITS student records management package is one of the University's core systems, and the system is upgraded regularly with modifications and new releases from the software supplier (Tribal). These are tested and implemented in the test environment by the SITS users. When the software has been tested thoroughly and approved, a change control is raised which then goes to a change control board, who will approve or reject the change. New developments are driven by the University's business and legal requirements.

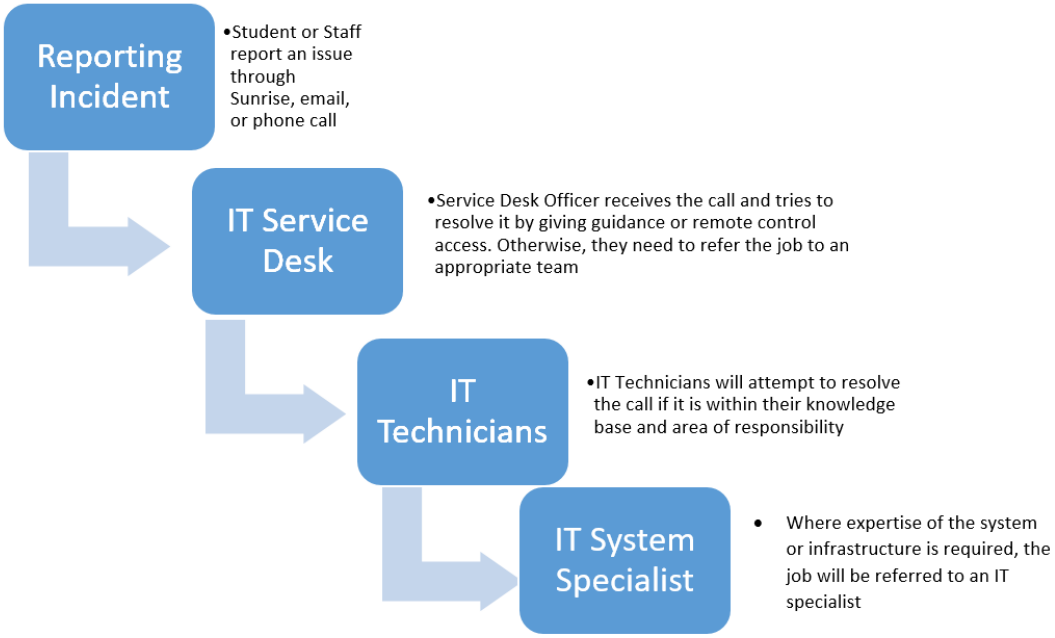

Figure 3. Incident Tracking by UoG IT Sevice Desk 2019

The general policy for the procurement of new software applications is that they should be based on web-enabled technologies that will assist in the development of a University-wide Managed Learning Environment (MLE). This principle guides procurement when the University has the opportunity to replace business systems through the annual IT capital programme.

UoG IT Service Desk functions: Sunrise is the main system used by the LTI staff to manage enquiries from students and staff. In addition, any enquiries received via the MyGlos Help Portal are redirected to the appropriate team. Different versions of Sunrise have been used by the University since the year 2000, but all with the same backend. With the latest version of this system, keywords can be used to select the problem categories and the problem is automatically assigned to appropriate support personnel.

The IT Service Desk performs a number of functions (Figure 2). It has the responsibility for all user account management as well as giving access to all University business systems such as Agresso and SITS. LTI is responsible for providing the basic "image" (i.e., software footprint) for all staff and student devices. A minimum of between 4-6 weeks is allowed to enable a thorough evaluation and testing of any new software application.

Figure 3 shows the escalation of a call through different levels of service expertise depending on the complexity/specialism of the problem reported. This systematic approach to tackling problems, combined with the application of dedicated human resources to solving Service Desk enquiries, has contributed to a significant improvement in response times and a more efficient IT service for the University's staff and students.

Support teams across the university's four main sites use IT Service Desk tools and the Sunrise support system. The IT Service Desk tools are an integral part of the Sunrise system, and were developed as a bespoke, standalone system for UoG. Some of its main functions are:

- Password reset
- Unlock accounts
- Create guest login for externals
- Provide access to shared drives
- Deploy software
- Change voicemail passwords

LTI uses the Sunrise system to log calls, update the call, and transfer the call to the appropriate support team. Service Desk officers have access to all communications across the University by searching for the Incident number (ID), call details, surname, forename, category, hub area, open date, network logon, global summary, priority, escalation level, assigned group, and first time fix. The call needs to be logged under the name of the person that reported the enquiry, which can be logged by network logon (staff number) or forename and surname. The category is selected based on the enquiry;

TABLE III.CYBERSECURITY CHECKLIST FOR SERVICE DESK MONITORING

	People Skills & Competencies	Process Requirements	Technology Deployment
Application security	• Respect for user privacy and confidentiality (access to sensitive data) • User systems knowledge • System administration skills and responsibilities • IT staff communication skills	• Systems documentation, user guide policy and procedures • Knowledge management (consistent terminology and definitions, amending and updating data) • Systems maintenance and update controls and procedures	• Authentication and access control in main business systems
Information security	• User awareness of criticality of data and information • Cybersecurity awareness programmes and briefings	• Data integrity policies and procedures • Information security recognized and managed as a continuous process	• Physical security mechanisms to protect assets and workplaces from unauthorized access • Data accuracy validation controls
Disaster recovery planning	• Clear management responsibilities for different Cyber threats	• Prevention and detection procedures • Threat and risk management processes to support vulnerability assessment • Incident tracking system and response plan	• Database recovery and back-up systems • On-site/off-site storage options
Network security	• User and IT professionals' awareness of Cyber threat via the networks. • Network administrator role with Cybersecurity responsibilities	• Network security controls and procedures, including password security • Control of network administration rights and privileges	• Firewall, antivirus and encryption programs for all physical and virtual servers, workstations, laptops, tablets, phones and mobile devices. • Appropriate Virtual Private Network utilization • Email server configuration and intrusion detection software • Resilient network architecture

for example, if someone reports an issue with email, Service Desk officers can search for emails and pick the correct category. The use of keywords and categories ensures that an enquiry is managed by the most appropriate team. Once the category has been selected, the system will automatically pick the first line team and referral team appropriate to the job.

All the operations of the Service Desk are now impacted by Cybersecurity issues, as has been highlighted by Whitman and Mattord. They note that technology has permeated every facet of the business environment in the last 20 years and that "the business is no longer static; it moves whenever employees travel for office to office"; and therefore "the security of the organisation also depends on the implementation of a multi-layered system" [17].

V. TOWARDS A CYBERSECURITY CHECKLIST FOR SERVICE DESK MONITORING

The Service Desk thus has a key role to play in the monitoring and reporting of Cybersecurity and this section draws together the different operational areas supported by the Service Desk at UoG to set out a rudimentary checklist for Cybersecurity (Table III). Cybersecurity is being marketed as a new software category, including Security Information Event and Management (SIEM) systems and Security Orchestration Automation and Response (SOAR) systems. These are in essence sophisticated reporting tools, sometimes involving machine learning, advanced statistical analysis and analytics software. Rapid7 [18], for example claim "security orchestration and automation helps teams improve their security posture and create efficiency—without sacrificing control of important security and IT processes". However, to

be of value, they still require the critical underlying data, and the "nuts and bolts" skills and competencies, processes and technologies that the Service Desk can monitor and help ensure are in operation to support the organisation's Cybersecurity. Once these building blocks are in place, then SIEM and SOAR systems can be introduced to provide overall automation and control.

an important competence for support staff. Confidentiality of data access is another important issue that is supported by UoG policy on data breaches, which allows recourse to relevant law enforcement agencies when appropriate. Technology related elements include Anti-Malware policy and associated software to protect the servers and workstations. UoG currently uses Sophos Anti-Malware.

TABLE IV. CYBERSECURITY CHECKLIST: DRILLDOWN DETAIL

Application Security: People Skills and Competencies
• User privacy and confidentiality (access to sensitive data) The concept of privacy is something all users must recognize and respect. In particular, sensitive data contained in business systems should not be divulged to other users or organisations unless authorized.
• User systems knowledge System users need to have appropriate levels of knowledge to be able to control and manage the data in a secure way. All users should be clear about their responsibilities, and how systems operations should be completed.
• System administrators and super-users Main business applications need systems administration and maintenance and this is increasingly located in end-user departments, requiring appropriate skills, knowledge and responsibilities. Super-users with expert knowledge of how an application works is another role often located in the user department, which may be vital in a disaster recovery or Cyber-attack context.
• IT staff communication skills Service Desk staff and other members of the IT team need the communication and vocabulary skills to explain technical issues in non-technical terms. This is important in explaining Cyber issues and may be critical in taking appropriate action in the event of a Cyber-attack.

In terms of Application Security, as defined in Section II, UoG has set up clear access control policies for its users in order to establish the rules, which govern the use of the University's accounts. These policies apply to all students and staff and to all of the University's IT systems, irrespective of how they are accessed. Staff receive privileged access, based on their role and the need for systems access. These People related issues (Table IV) are complemented by policies setting out related Processes, notably for software documentation, user guides and associated procedures. Technology measures include password authentication and systems audits and logging capabilities.

As regards Information Security, Meyers [19] has observed that most security breaches occur at user level, and result from human actions. This has helped shape UoG policy, providing basic security awareness to all users and educating staff and students on, for example, Pishing emails, spam collection etc. A recent survey of Cyber awareness training [20] found that only 11% of organizations continuously train employees on how to spot Cyber-attacks, 24% admit to monthly training, and 52% perform training only quarterly or once a year. The report concludes, "Humans can be either a first line of defense, or the first line that Cybercriminals seek to exploit when they attack an organization. Their behavior and the culture you influence greatly impact the effectiveness of your overall Cyber resilience strategy" [20].

The ability to communicate technical issues to non-technical people in a clear and effective manner has become

If the anti-malware software finds a problem it automatically sends an email to designated members of the First Line Support Team as well as specific second line support staff (e.g. the Information Security and Cyber Developer). With portable devices, there is a greater risk of loss, or infection from the malware, and UoG register all such devices to an accountable owner who is made responsible for security issues. All relevant UoG security policies are applied to these devices to provide protection against unauthorised use.

For Disaster Recovery planning, UoG has set out the rules to govern the ways in which the university makes copies of the data held within its various IT systems. In the event of data loss, caused by an 'incident' (major or minor), data can be restored from the back up and normal service can be resumed. Such 'incidents' include systems crash, ransomware attacks, natural disasters (fire, flood) and catastrophic failure. Processes are in place to identify and recognise the problem, make an initial assessment and communicate the issue to all users. Identified managers are responsible for identifying the nature of the incident, point of origin, determine the intent and identify systems compromised. LTI managers must evaluate the solution and monitor it to determine the outcome. Backups for compromised systems may be used and managers need to review and report on the incident with recommendations for future reference. The technology used for back-up operations does not provide archiving or permanent storage. The storage of data according to specified retention schedules is achieved through management of storage within the online systems. All

data held within the Storage Area Network, the virtualised guests and the network file stores is backed-up daily. Initially these back-ups are stored on disc and then transferred to tape. At regular intervals, the tapes are removed to secure storage areas. Both the discs and the tape library are housed separately from the 'live' data, and back-up tapes are encrypted to safeguard data.

Network Security overlaps several of the policy and technology elements discussed above. IT Administrators have specific access rights to the networks and are responsible for ensuring appropriate business continuity measures are in place to protect against events, which might otherwise result in loss of service. Default passwords must be changed the act of changing password is recorded. The effective management and integrity of the networks is supported by firewalls and anti-malware software.

VI. DISCUSSION

This section draws on the case study material discussed above to address the research questions set out in section II.

RQ1. How have the support requirements of Helpdesks and Service Desks evolved over the past thirty years?

Thirty years ago, the need for IT support in major organisations were somewhat different from those of today. There was no significant use of the internet and very few mobile phones or laptops. There was no Windows - MSDOS was the main operating system for PCs. There was no SKYPE, no viruses and no Wi-Fi, but Intel chip-based PCs had established themselves in most organisations and hard-wired LANS linked them to server PCs and mini-computers. Most business systems were bespoked in-house – the age of integrated packaged software was just around the corner.

However, despite the expansion in the range of technologies that Service Desks are now called upon to support, there was arguably more variety in the range of products that needed supporting in each technology category. For example, the Glaxo Helpdesk supported five different word processors and several spreadsheets and graphics packages. The market was still evolving with many competing products and no obvious standards. Presentation graphics systems and videoconferencing also needed support, along with bespoked computer-based training packages in the era before on-line help functions for many software products.

There is now a greater range of technologies to support, but there are clearer standards and more obvious choices within each category. It is thus critical that the central support function has clear policies and makes product choices in each technology area. At Glaxo, despite the lack of standards in end-user software, the IMD Director was adamant that only Intel chip based PCs would be permitted in the company, and this has parallels with UoG's non-support of devices not obtained through the University procurement system. In recent years, there has been a clear imposition of standards and product choices at the University as central IT strategy and policies have taken precedence over departmental initiatives.

Over the time duration between the two case studies, the Helpdesk function has evolved and adapted to changing requirements and developments in technology. The concept of support has also evolved, with Helpdesks or Service Desks increasingly seeing computer users as "customers", but at the same time end-users taking some responsibility for systems ownership, data maintenance and training. The super-user and data maintenance specialists have emerged as key link personnel between the computer user-community and central IT support.

RQ2. How has the Service Desk developed in response to the need for Cybersecurity?

Hila Meller, BT's vice president for Security, Europe, noted recently "security needs to be a concern across the whole organisation, not just the remit of the IT department. Everyone needs to play their part, to stop shadow IT and ensure data breaches don't happen" [21]. Nevertheless, the Service Desk has a key role to play in this endeavor, and Cybersecurity is now a major issue for Service Desk operations. Cybersecurity itself consists of "technologies, processes and measures that are designed to reduce the risk of a Cyber-attack (which is conducted through the deliberate exploitation of systems, networks and technologies)" [11]. This underlines the vast scope of Cybersecurity and points up the new capabilities, knowledge and skills required of the Service Desk personnel, who must play a key role in prevention, tracking and resolution of Cyber-attacks.

Digitalisation and the "disruptive technologies" pose new challenges. David Carvalho, Global CISO at OCS Group, has remarked that the Internet of Things (IoT) represents another area of emerging vulnerability. "IoT is everywhere, smart cameras, dumb cameras, all sorts of sensors, SCADA devices, and companies that use PLCs (programmable logic controllers). The whole world is producing IoT devices with few or no regulations at all" [22].

This is producing new demands on the training and reskilling of Service Desk staff. Mannie Romero, the executive director in the office of the CISO at Optiv, recently observed that "people who were network people in the past and are used to running discovery scans and doing things on the network and the system, now have to move up the stack to the applications and start learning APIs in AWS, Azure, and other cloud infrastructures. The situation is only going to get more challenging, as artificial intelligence, robotics, machine learning, and IoT become more prominent and widely deployed" [22].

In practice, this has seen Cybersecurity develop as a discipline or specialism in its own right in the business and consultancy fields, and as a major component of an organisation's operations, sometimes with a CISO reporting at Board level. For the Service Desk, as noted above, this has produced new and rapidly evolving demands on people skills and competencies. A recent report on Cybersecurity concludes, "Having the necessary technical personnel in place is one of the most important — and most difficult — elements of any organization's security posture. Organizations of all sizes and maturity levels struggle to

attract and retain the right mix of people to help manage and secure their computing environments" [23].

In terms of technology deployment, Cybersecurity technology is becoming increasingly sophisticated. Threat prevention, for example, is a critically important component of a Cybersecurity strategy, and most organizations invest significantly in security controls and processes in this area. Oltsik notes, "Tools like endpoint security software, web threat gateways, and IPSs are designed to identify and block an assortment of activities deemed to be malicious". He adds, "Beyond blocking known malicious behavior, organizations must collect, process, and analyze internal and external data, identify and investigate suspicious activities, and remediate problems quickly before minor issues become major data breaches. The processes, tools, and personnel used for these tasks are generally referred to as security analytics and operations" [24]. Although there are some similarities in the business systems and desktop tools used by the two organisations in the two case studies spanning a thirty-year time gap, the technology requirements for addressing Cybersecurity issues are now on a different level. In the 1980s, the advent of the PC and the growth of end-user computing was the catalyst for the development of the Helpdesk with new skills requirements and supporting technology. In this decade, it has been the emergence of Cybersecurity issues that have driven a similar step change in Service Desk operations and staffing.

VII. CONCLUSION

The old Helpdesk is now increasingly seen as part of a broader Service Desk function, with service being defined as "an approach to IT service management that emphasizes the importance of coordination and control across the various functions, processes and systems necessary to manage the full lifecycle of IT services" [25]. This definition is often applied in the context of a third party service provider, but is also relevant to in-house IT service provision. At UoG, the Service Desk is the customer facing front end of all IT services, which are measured against stipulated service level targets defined in service level agreements. This aligns with the IT Infrastructure Library (ITIL) concept and definition of the IT Service Desk as the single point of contact between the IT function and users, which manages incidents and service requests, and handles communication with users. There is also a more subtle change in that the service is seen as supporting business processes and people capabilities along with the pure technology elements. The Service Desk now focuses on delivering high quality customer service to end-users, whereas the Helpdesk was more concerned with incident management and resolving problems related to IT in the organization.

The range of different technologies supported by the Service Desk has seen developments in its own support technology. In addition, the requirements set out in service level agreements have meant that Service Desks need to increase end-user satisfaction levels by responding to the incidents and problems within stipulated response times. To support this increase in customer service levels, support technology has become more sophisticated, involving elements of knowledge management and artificial intelligence.

Over and above this, however, as Peppard [26] has noted, the role of people skills and capabilities in delivering a successful Service Desk operation remains critical. In the context of Cybersecurity, this is true in its widest sense. As Bechkoum notes, "having an effective Cybersecurity culture within your organisation is vital" [27]. The key is to bring together relevant IT and security teams united through the actions of an empowered Service Desk. If the organisation is able to do this effectively, detecting the early warning signs of a potentially serious threat becomes easier. Such a preventative approach is likely to prove the most effective security model for most organisations. Despite advances in technology support systems, a fully automated Service Desk function remains some years away. Computing Research [2] have concluded "as the Internet of Things gathers pace, those data volumes will explode into something which we are all collectively struggling to even imagine. The role of AI and machine learning in security solutions in this sense is not a matter for debate. They simply have to play a role – and as data volumes grow, the role for AI will grow with it. However, for now and the foreseeable future, the role of AI in Cyber security is likely to remain as a partnership with humans. Neither can quite manage the task alone."

REFERENCES

[1] M. Rezaeian and M. Wynn, "The Evolution of the Customer-Centric Helpdesk: Two Case Studies" *The Eleventh International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services* (CENTRIC 2018) IARIA, Nice, France, 2018, pp. 7-13.

[2] Computing Research. (2016, Nov. 16). *Enterprise security review* [Online]. Available: https://www.computing.co.uk/ctg/news/2478143/computing-enterprise-security-review-2016

[3] IGI-Global Newsroom. (2019, Feb. 18). *How to prevent your phone from spying on you through the latest cybersecurity advancements* [Online]. Available: https://www.igi-global.com/newsroom/archive/prevent-your-phone-spying-you/4066/

[4] Computing (2019, Jul. 8). *British airways faces £183m GDPR fine over last year's security breach* [Online]. Available: https://www.computing.co.uk/ctg/news/3078541/british-airways-gdpr-183m-fine-payments-security?utm_source=Adestra&utm_medium=email&utm_content=&utm_campaign=CTG.Daily_RL.EU.A.U&im_edp=1415226d3d7959ccd15603%26campaignname%3DCTG.Daily_RL.EU.A.U&utm_term=Higher%2FTertiary%20Education&im_company=UNIVERSITY%20OF%20GLOUCESTERSHIRE&utm_term=1000%20to%201999

[5] M. Wynn, "The business benefits of pc office systems and end-user computing at Glaxo Pharmaceuticals, 1984 – 1988", *Journal of Information Technology*, vol. 4, issue 1, pp 17-29, Mar 1989.

[6] D. Bridge and A. Dearden, "Knowledge based systems support for help desk operations : A Reference Model", Dept of Computer Science University of York [Online], April 1992. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.47.5118&rep=rep1&type=pdf /2018.07.22

[7] L.Gonzalez, R. Giachetti, and G. Ramirez, "Knowledge management- centric help desk: specification and performance evaluation", *Decision Support Systems*, vol. 40, pp. 389-405, 2005.

[8] U. Sood, " 7 Essentials for a top-performing IT help desk", GCN Executive Roundtable Cloud [Online], March 30, 2017. Available: https://gcn.com/articles/2017/03/30/help-desk-essentials.aspx/

[9] National Institute of Standards and Technology, Glossary of Key Information Security Terms. NISTIR 7298 Revision 2, U.S. Department of Commerce, 2013. Available: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[10] Economic Times, "Definition of Cyber Security". Available: https://economictimes.indiatimes.com/definition/Cyber-security

[11] ITGovernance. (2019, Nov. 15) *What is cyber security*[Online]. Available: https://www.itgovernance.co.uk/what-is-Cybersecurity

[12] A. Bryman and E. Bell, *Business Research Methods*, 3rd edition, Oxford: Oxford University Press, 2011.

[13] M. Saunders, P. Lewis, and A. Thornhill, *Research methods for business students*, 5th ed.England: Pearson Education Limited, 2012

[14] M. Wynn and L. O'Callaghan, "Quality graphics at Glaxo pharmaceuticals", *Training Technology*, vol. 1, issue 4, pp. 18-20, Apr 1988.

[15] R. K. Yin, *Applications of Case Study Research*. 3rd ed. London: SAGE Publications, Inc, 2012

[16] M. Wynn, "Computerised training solutions at Glaxo", *Interactive Learning International*, vol. 4, issue3/4, pp. 73-80, Sep1987.

[17] M.Whitman and H.Mattord, *Managing information security*, 4th ed, Stamford, CT, USA: Cengage Learning, 2014.

[18] Rapid7. (2019, Nov. 15). *Security orchestration and automation playbook - Your practical guide to implementing a SOAR solution* [Online]. Available: https://www.rapid7.com/info/security-orchestration-automation-playbook/

[19] M. Meyers, "Don't be hacked: 5 cyber security skills your IT team needs to master", Udemy for Business IT instructor and President of Total Seminars, Feb 27 2019. Available: https://business.udemy.com/blog/Cyber-security-skills-it-teams/

[20] Mimecast. (2018, Nov. 14). *Employees behaving badly? Why awareness training matters* [Online] Available: www.mimecast.com

[21] H. Meller, "Don't let security cloud your views on digital transformation", British Telecommunications plc, November 2018. Available: www.bt.com/risk-reward-cloud

[22] Tenable. (2018, Jan. 12). *Reducing Cyber Exposure from Cloud to Containers* [Online]. Available: www.mightyguides.com

[23] CrowdStrike Services. (2019) *Guidance for Maturing Cyber Defenses* [Online]. Available: www.crowdstrike.com/

[24] J. Oltsik, "Cybersecurity Analytics and Operations in Transition", Enterprise Strategy Group, July, 2017.

[25] The Stationary Office (TSO), *ITIL Foundation Handbook*, IT Service Management Forum, 2012.

[26] J. Peppard,"Managing IT as a portfolio of services" *European Management Journal*, vol. 21, issue 4, pp. 467–483, 2003.

[27] K.Bechkoum, "Building a Cybersecurity culture for your business", University of Gloucestershire [Online] , Feb 25, 2019. Available: https://medium.com/@bechkoumkamal/building-a-Cybersecurity-culture-for-your-business-60bb183a7493