****

9B18E019

Malus analytics international: combatTing the menace of shadow it

Owen Hall, Jr. and Erik J. Krogh wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

*This publication may not be transmitted, photocopied, digitized, or otherwise reproduced in any form or by any means without the permission of the copyright holder. Reproduction of this material is not covered under authorization by any reproduction rights organization. To order copies or request permission to reproduce materials, contact Ivey Publishing, Ivey Business School, Western University, London, Ontario, Canada, N6G 0N1; (t) 519.661.3208; (e)* [*cases@ivey.ca*](mailto:cases@ivey.ca)*;* [*www.iveycases.com*](http://www.iveycases.com)*.*

Copyright © 2018, Ivey Business School Foundation Version: 2018-12-21

At the Malus Analytics International (MAI) board meeting in August 2018, held in Denver, Colorado, the primary focus was to establish a response to address the rapidly increasing impact of “Shadow IT” (information technology) on the operating performance of MAI’s clients.

MAI’s chief executive officer, Dr. Chelsea Bordon, began the meeting by providing an overview of Shadow IT and summarizing the feedback from MAI’s client base. Bordon explained, “Shadow IT is usually defined as devices, data, systems, software, and services outside the control of central IT.” She added that MAI’s customer service department was receiving an increased volume of requests for support from MAI’s nearly one thousand clients on a worldwide basis regarding the Shadow IT problem.

Dr. Mike Champion, the board’s vice-chairman, weighed in and asked for a more descriptive characterization of the so-called Shadow IT issue. MAI’s chief information officer (CIO), Dr. Edward Keller, provided more details. Keller reported that in a recent telepresence meeting with 20 of MAI’s top clients, the refrain was essentially that clients were experiencing more data breaches, which were due in large measure to employees’ unsanctioned use of Software as a Service (SaaS) applications (apps). Keller explained that he had reassured the meeting participants that MAI would be developing an appropriate plan to address the problem. Keller then advised the board that the deployment of a Shadow IT amelioration plan would both significantly improve customer loyalty and boost revenues.

Bordon thanked Keller for his report and indicated to the board that MAI’s research department had been working on a blended Shadow IT strategy, combining the best practices of central IT oversight without overly restricting end-users’ innovation and flexibility. As the board meeting concluded, Bordon directed Keller to finalize the plan and report back at the next board meeting.

Cloud Computing and the Rise of Shadow IT

Cloud computing was one of the most significant developments affecting the global business marketplace because it provided the opportunity for firms to lower their IT expenses. Cloud computing, also known as on-demand computing, provided computing resources (both hardware and software) that were delivered as a remote service over a network (typically the Internet) to host and manage a user’s data, software, and computational activities. Cloud computing offered a variety of benefits, including a reduction of the data centre footprint, access to the latest technology provided and maintained by the cloud provider, and the ability to ramp capacity up or down based on demand. Cloud providers managed the infrastructure and platforms on which the applications ran.

The cloud market was segmented into three broad sectors: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS consisted of network and storage capabilities complemented by scalable computing resources. IaaS customers could establish cloud-based data centres that had the same technologies and resource capabilities as a traditional data centre without having to invest in capacity and maintenance. PaaS was a category of cloud computing services that offered clients a vehicle to develop and manage applications without the costs associated with building and maintaining the required internal infrastructure.

SaaS, which was commonly referred to as on-demand software, was usually priced on a pay-per-use basis, as opposed to purchasing a perpetual licence, which historically had been the norm. SaaS vendors were offering more customization and flexibility in their software offerings compared with traditional on-the-premises suppliers. Furthermore, some SaaS providers furnished some of their products and services at no cost as a means of generating sales for their other products and services. In a variation of this approach, called the “freemium model,” software with limited functionality was provided free, and fees were charged to enable enhanced capabilities. Overall, observers estimated the cloud computing market would surpass one trillion dollars by 2024.[[1]](#footnote-1)

Cloud computing had emerged as a new way for organizations to significantly cut their technology expenses while boosting organizational performance and productivity. As storage, services, and applications moved to the cloud, corporations were seeking new and less expensive ways to deliver and manage their IT services. The ongoing growth of cloud computing, however, was one of the driving factors in the rise of the Shadow IT menace.

An increasing number of employees were using BYOD (bring your own device) as their instrument of choice for accessing the cloud and communicating with customers, but doing so left many organizations vulnerable. Specifically, because end-users were downloading and uploading content to their own devices, the opportunities dramatically increased for malware, viruses, and hacks. Further, when employees used their devices on unsecured networks (e.g., at coffee shops) to access the organization’s cloud resources, the firm’s data were made vulnerable and exposed to significant risk. Having employees use their own communication devices also raised privacy concerns, not only for the end-users but also for their employers. Social messaging apps were another growing opportunity for organizations to maintain ongoing customer contacts and to improve the customer experience; however, this growing trend again opened the firm to enhanced cyber security risks and increased the central IT monitoring of employees’ personal information.

Shadow IT allowed end-users to bypass central IT solutions and develop their own customized approach to the specific task at hand. End-users strove to work around IT roadblocks (a concept known as “local optimization”), but the CIO considered this approach to be a suboptimal allocation of resources. CIO oversight could reduce duplication of applications, and oversight could promote integration and interconnectivity between applications through a process of ongoing communications with the end-user community. For example, operating a single help desk optimized both customer service and trouble ticket tracking, and it allowed for root-problem analysis and remediation, which could provide significant cost reductions.

Consolidated data centres and data storage were advantageous on multiple levels (e.g., reducing the digital footprint). Institutionally provided IT improved supportability, fostered project resource flexibility, and allowed end-users to focus on the tasks at hand rather than developing their own IT solutions. As an added insurance policy, some organizations were adopting firm-based devices, known as “choose your own device” or CYOD, which had the capability to isolate personal applications and data in a secure on-device system.

THE SHADOWY WORLD OF SHADOW IT

For several decades, CIOs had battled Shadow IT, defined by many IT pundits as “devices, data systems, software and services outside the control of central IT.”[[2]](#footnote-2) The reasons for these concerns included unvetted IT brought into an organization, which could result in numerous problems, including cyber security breaches, noncompliance with regulatory requirements, duplication of existing applications, lack of IT help desk support, user-built applications not coded to institutional standards, applications that did not integrate, and inefficient use of the IT budget.[[3]](#footnote-3) However, in a growing digital economy, end-users had more IT options available to them than ever before, and recent studies suggested that these users were increasingly using IT not provided or sanctioned by their CIO. For example, 64 per cent of employees still used unapproved apps in the workplace even though this problem has been known for many years.[[4]](#footnote-4)

The CIO’s traditional, vertically integrated organizational structure provided a one-stop shop for applications, infrastructure, cyber security, database, architecture, and support. As IT became ever more essential for the realization of enterprise objectives in the digital economy and demand for IT-enabled capabilities increased, the timely fulfilment of IT needs was often beyond the CIO’s capacity. The unmet IT needs of organizational units had driven them to seek their own IT solutions and, as a result, diminish the CIOs’ control over the corporate IT environment.

A common complaint from the end-user was that the CIO did not deliver requested solutions in a timely manner and the said solutions were not based on the latest, cutting-edge technology. End-users also believed that they were handcuffed by outdated IT policies and processes, and, in many instances, end-users did not need the support of centralized IT. In this regard, the CIO needed to weigh the impression of being an institutional enabler and embracing user-sourced IT versus the perception of being an institutional obstacle, perceived by end-users as frustratingly slow and outmoded. If the CIO could not meet the IT needs of its business constituents, end-users then had an incentive to source IT on their own, circumventing the CIO in the process. CIOs reacted to this phenomenon in various ways, from clamping down on Shadow IT to assuming a more accepting posture. As IT affordances became increasingly available, the notion that the CIO was responsible for all things IT had become doubtful.

Identifying the various manifestations of unauthorized IT was the first step to understanding how best to address the Shadow IT challenge. Unfortunately, no one had developed an acceptable definition of corporate, non-sanctioned IT use. Adding to the confusion were implicit references to unsanctioned IT use, such as users accessing SaaS cloud apps without the approval of the CIO; the unsanctioned implementation of PaaS and IaaS by business end-users; unsupervised Web 2.0 and social media use, including blogs, social networking, mashups, and video sharing; and end-user-developed digital capabilities (i.e., new applications or modifications of existing applications) (see Exhibit 1).

COMPANY BACKGROUND

MAI, which was founded in 2014, provided a variety of analytics-based services via the cloud, including predictive algorithms for forecasting sales trends based on customer behaviours and external economic factors. MAI’s product and service offerings also included an extensive security suite to address the ongoing challenges associated with data breaches.

MAI had experienced significant revenue growth over the previous few years, with sales approaching US$160 million[[5]](#footnote-5) annually. MAI’s business model was based on the premise that the demand for cloud computing solutions would continue to grow as companies sought ways to lower their IT expenses.

MAI provided both consulting services to assist in transitioning to the cloud and priority-based predictive analytics systems on a SaaS basis. MAI’s cloud computing strategy for its clients was based on four characteristics: A strong selling point for MAI’s SaaS analytics services was its suite of analytics development tools that allows end-users to rapidly get answers to ad hoc questions. MAI encouraged clients’ end-users to use these tools to develop their own applications to exploit the wealth of data now available on the cloud. While many end-users did indeed utilize these tools, there were multiple “super users” who figured out how to access data on the cloud using unsanctioned means such as Excel spreadsheets and homegrown applications.

As MAI’s push to move its clients to the cloud gained traction, an uptick in the unsanctioned use of IT had increased the exposure of a number of clients to a variety of security risks as uncovered by the clients’ own cybersecurity departments. Many of the clients’ CEOs thought that this uptick in Shadow IT was a result of the move to the cloud, and they held MAI responsible.

MAI needed to step in and help their clients resolve the situation. Unless the company took quick action, MAI could experience a significant client backlash, resulting in a reduction in both revenues and clients. Since nearly 75 per cent of MAI’s revenues came from the consulting division, any reduction in clients could have a major impact on the firm’s future financial viability.

DEVELOPING A NEW APPROACH

In this context, Keller, MAI’s CIO, had set about formulating a revised cloud-computing approach that could be suggested to MAI’s clients—an approach that balanced the legitimate needs of end-users with the overall perspective of the CIO, especially in terms of security concerns.

Keller’s first step was to survey both end-users and the CIOs from a subset of MAI’s client base. The results, not surprisingly given the prior feedback, revealed two fundamentally different perspectives. Almost all of the CIOs interviewed weighed in by expressing their number one concern: cybersecurity. Many of them were also frustrated that end-user self-sourcing of IT was a great deal more expensive to the company than buying IT at scale through a centralized IT procurement office. Fragmented IT also made user support more difficult. A third issue cited by multiple CIOs was a conflict over sourcing IT. The CIOs felt that their department possessed the IT expertise and that the CIO should be responsible for technology leadership; the business units should focus on what they did well, not on sourcing IT. From the perspective of the end-users, the dominant issues were, by and large, completely different. End-users viewed CIOs as obstacles and providing poor solutions. End-users considered themselves self-sufficient and were unaware of CIOs’ regulations.

None of these factors surprised Keller, given his nearly 30 years of experience in the IT community. Keller was also aware that many of MAI’s customers were expanding their use of social messaging apps as yet another opportunity for organizations to maintain ongoing customer contacts and improve the customer experience. However, the use of social messaging simply opened another cyber security challenge.

Keller understood that MAI’s initial approach had increased the duplication of applications by allowing end-users at each of its clients to develop their own self-styled IT solutions. Experience suggested that, in most situations, this behaviour would lead to suboptimal use of the client firm’s resources.

Making the case for technological leadership at the CIO level was another area not addressed by MAI’s initial plan. The notion was that institutionally provided IT improved supportability, fostered project resource flexibility, and allowed end-users to focus on the task at hand instead of developing their own IT solutions. However, end-users often viewed solutions provided by central IT as being ineffectual in terms of both timelessness and costs. Furthermore, as the survey results revealed, end-users were generally unaware of central IT’s regulations and had differing views on organizational culture, especially in terms of promoting innovation.

Keller’s next step was to try to coalesce these two different perspectives. He decided to use a causal loop diagram (CLD) approach. CLDs provided a useful methodology for helping to resolve qualitative-based conflicts, such as those encountered in the survey data. CLDs offered a visual perspective on how different factors (e.g., classifications) were interrelated, and how they had been widely used across a variety of organizational applications, including Shadow IT. Basically, CLDs consisted of nodes and edges, with the nodes representing the identified factors and the edges connecting the factors.

CLDs were useful for depicting, in a simplified manner, how systems worked. The diagrams featured two types of loops: *positive*, or *reinforcing* loops; and *negative*, or *balancing* loops. Reinforcing loops were depicted as moving in a clockwise direction, while balancing loops moved counter-clockwise. These loops could be conceived of as a dialogue between two competing interests. The reinforcing loop sought to extend previous limits, while the balancing loop pushed back when the reinforcing loop had “gone too far.” Reinforcing feedback represented goal-seeking, and balancing feedback represented stability-seeking behaviour. For this application, the reinforcing loops represented the end-users and the balancing loops portrayed the CIOs.

Armed with these new insights, Keller decided to formulate a plan that balanced the competing interests and could be communicated to MAI’s client base. He concluded that communication and relationship-building represented a first good step in attempting to ameliorate the basic differences between the two groups. He then set about developing a PowerPoint presentation that was to be delivered at the board’s next meeting, as Bordon had directed.

Exhibit 1: Shadow IT Examples

|  |  |
| --- | --- |
| **Category** | **Examples** |
| BYOD | Mobile phones, tablets, notebook computers |
| End-User Development | Spreadsheets, personal databases, user-developed applications (UDAs) |
| File Sharing and Storage | Consumerized file-sharing apps |
| Group Collaboration | Cloud-based document applications, team collaboration apps |
| Personal Productivity | Calendaring, note-taking and organizing apps |
| Public Cloud IaaS | Cloud platforms that host data centre structures |
| Public Cloud PaaS | Cloud platforms that provide infrastructure needed to deploy UDAs |
| Public Cloud SaaS Apps | Cloud platforms that allow users to access applications |
| Web 2.0/Social Media | Blogs, microblogging services, wikis |

Note: apps = applications; BYOD = bring your own device; IaaS = Infrastructure as a Service; PaaS = Platform as a Service; SaaS = Software as a Service.

Source: Created by the case author.

1. *Global Cloud Computing Market Forecast 2019–2024*, Market Research Media, January 2018, accessed July 4, 2018, www.marketresearchmedia.com/?p=839; All currency amounts are in US dollars. [↑](#footnote-ref-1)
2. “What Is Shadow IT?,” Cisco, accessed September 23, 2018, www.cisco.com/c/en/us/products/security/what-is-shadow-it.html. [↑](#footnote-ref-2)
3. Robert Dimicco, “Gartner Report Says Shadow IT Will Result in 1/3 of Security Breaches,” Cisco blog, June 22, 2016, accessed July 4, 2018, https://blogs.cisco.com/cloud/gartner-report-says-shadow-it-will-result-in-13-of-security-breaches. [↑](#footnote-ref-3)
4. Natalie Lambert, “Shadow IT Is Sabotaging Your Business—Here’s How to Stop It,” IT Pro Portal, January 27, 2017, accessed July 4, 2018, www.itproportal.com/features/shadow-it-is-sabotaging-your-businessheres-how-to-stop-it. [↑](#footnote-ref-4)
5. All currency amounts are shown in US$. [↑](#footnote-ref-5)