Microsoft

Consumerization and Security

Effective Security Practices Series

Employee-owned smart phones, laptops, and other mobile devices have entered the IT security landscape - bringing both utility and risk. This trend is a part of a larger movement to bring consumer devices, tools and services into business environments known as consumerization. Consumerization can be a polarizing issue in corporate IT. Cost pressures, employee preferences, and new technologies build a compelling case for consumerization, but concerns linger over security, audit and governance. This paper focuses on the current security risks of consumerization and effective practices businesses are using to manage it based on interviews with security executives from some of the world's largest corporations.

Herbert H. Thompson, Ph.D.
Chief Security Strategist, People Security

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Preface

Information security is a very dynamic field: legislation keeps changing, technology keeps evolving, and the attacker community continues to become more sophisticated. This turmoil has forced security practitioners to think creatively to address some very difficult problems. Much of this innovation has been locked away within corporations as they have made isolated progress on issues like security metrics, security risk management frameworks, and security policy. In order to address this discrepancy, Microsoft commissioned a whitepaper series to share key security innovations. Whitepaper topics came from participants in Microsoft's CSO Council - a semi-annual gathering of security executives from leading global organizations who serve as advisors to Microsoft's Trustworthy Computing Group.

Our goal is to share practices "from-the-trenches" that address some of the toughest problems in security. After numerous interviews, discussions, and debates with these though leaders, a collection of effective practices emerged. While much remains to be done, we hope that these whitepapers fuel the discussion and help facilitate further sharing in the field of IT security.

Understanding Consumerization

Some key shifts in the IT environment have led to user-owned devices being deployed for business purposes. This move to consumer devices and services falls under the umbrella of "consumerization." Currently, consumerization is a divisive issue among large enterprises. While some have rejected (or at least tried to postpone) consumerization--citing compliance, governance, and control concerns--others have embraced it. The reality is that some degree of consumerization is probably unavoidable. In this paper we look at effective practices that businesses are using to manage consumerization today.

In preparing this paper we talked with several Chief Information Security Offices (CISOs) and security architects in large enterprises. There was a general feeling of inevitability around consumerization among most respondents. Many believed that consumerization had already occurred in their businesses even in cases where the business had strict policies requiring employees to use corporate-managed devices for work functions.

Consumerization is happening in many different ways. The first is the use of consumer websites and services to get work done. Hotmail, Linked-In, Twitter and other web tools all fall under this category. The other is a move toward employee-owned hardware, such as smartphones and laptops. Smartphones were the most commonly cited employee-owned/managed device that had made it into business workflows. There are several factors driving this. Productivity demands on employees have increased over the last decade, partly due to layoffs and downsizing. There is a growing expectation for employees to deliver anytime, anyplace. While businesses push for increased productivity, they may not be able to justify investments in best-of-breed productivity tools such as smartphones for employees. Many employees already have the smartphones and laptops needed to meet business demands at home and they want to integrate them with their work life. Mounting pressure from both employee and corporation has pushed businesses to consumerize.

Consumerization in Practice

Bringing employee-owned and managed devices into the business raises some important security questions. The most commonly cited concern by the group of enterprise security executives interviewed was governance. If the company doesn't own the device, there are open questions around compliance and audit. The second concern was around e-discovery. There was some unease around being able to examine and possibly subpoena

an employee-owned device in the case of legal proceedings. For e-discovery there was also a concern that retrieving business data from an employee device might inadvertently retrieve personal data that might be sensitive and clearly not company property. A third concern was over the general security and control of data. For corporate-owned devices, configurations can be set and enforced, in addition to installing security software and monitoring software updates. For employee devices, this lack of enforceable security controls raised concerns that corporate data might be put at increased risk. In the case of smartphones, many companies were able to mitigate this by requiring phones that supported ActiveSync and agreeing to some amount of corporate control over data along with the ability to remotely wipe the phone.

For those companies that had policies prohibiting employees from using their own devices in the workplace, there was a general belief that users routinely violated policies, sometimes driven by productivity needs. In one example a respondent pointed out that Blackberry devices were only supplied to managers, but other employees would routinely either use their personal smartphones or in some cases purchase a new smartphone to keep up with corporate email. Several respondents noted that employees don't want to bring two devices with them on the road, yet they need to be connected professionally and personally.

Most respondents are working on infrastructure changes to better support consumerization. The most commonly cited first steps towards hardware consumerization were employee-owned smartphones. Some had begun to implement technology and policy changes to support personal laptops while others resisted this move. Below are some specific cases that offer insight into how the CISOs interviewed are dealing with consumerization:

Case 1: Integrating employee-owned laptops

A large financial services company is wrestling with consumerization in an environment that was traditionally locked down with corporate-issued laptops and smartphones (in this case Blackberry devices). Some executives had started to bring in other smartphones as well as Apple and Windows 7 laptops, departing from the corporate standardized Windows XP desktops/laptops. This pushed IT to look into virtual laptop solutions where the business could control and isolate a work image on an employee-owned laptop (both online and offline). The hosted image would sync documents with corporate

servers (when online) and enforce a boundary between the corporate workspace and the laptop host.

Case 2: An enterprise embraces consumerization

A large consumer products company has embraced the idea of consumerization. The process began several years ago and consumerization has now been woven into the fabric of IT. New offices have basic routers and machines that connect directly to the Internet with tunneling to the corporate network for some services. Email is hosted in the cloud and accessible from any machine over the web. Employees use their own smartphones to retrieve corporate email. Employees are given a stipend to help maintain and support their personal laptops, moving the burden of general support outside of corporate IT. Additionally, the company is in the process of establishing relationships with large electronics resellers to provide in-person and phone support for employee laptops under contract.

Case 3: Limited Integration of employee-owned smartphones

A large transportation company was under increasing pressure from employees, many of whom were mobile, to use their personal smartphones to retrieve corporate email. The company introduced a policy that allows employees to use personal smartphones as long as they supported ActiveSync for secure email transmission/storage and remote wipe in case of loss. Employees wanting to use these smartphones did so with the agreement that corporate IT could issue remote wipe commands.

Case 4: Cutting costs through consumerization

A large business services company was pushed towards consumerization as a way to cut costs. Moving some key business services to the cloud led to an environment which better supported employee-owned devices. Email services were moved from the company's servers to the cloud. This helped the company save on storage and power costs, and avoid a significant capital expenditure on equipment upgrades. Additionally, the company moved some of its security services to the cloud, piping web traffic through externally managed systems, which saved a planned investment in additional hardware. These two shifts led to an environment where the company still had visibility into and control of data flowing out of employee owned devices using cloud-based proxies.

Conclusion

While consumerization continues to be a polarizing issue for large corporations there is a general feeling of inevitability. In talking with security executives and architects we found that the needs and expectations of corporations are outpacing investments in employee devices. Employees see opportunities to be better at their jobs by filling the gap with personal devices. As supporting security technologies come to market, there is a mounting case for corporations to acquiesce. Several open questions around security and governance still remain but the traditional separation of personal and business is being trumped by a need for operational efficiency. The rise of cloud security services, more granular remote access to corporate resources, a faster consumer technology adoption cycle, and a desire to move maintenance costs for devices downstream to employees are all building support for consumerization. One of the biggest barriers is a lack of information sharing about battle-tested policies and practices that support consumerization safely. This paper was written to help add to that discussion.