ABSTRACT

The use of virtual worlds and social media has grown to the point that more than one-quarter of the world’s population utilize it in some manner. Security and privacy concerns regarding the use and capabilities of current and emerging technologies such as gaming, blogging, podcasting, virtual meetings, virtual worlds and Web 3.0 is examined. Security and privacy concerns are investigated in the context of exploits, vulnerabilities, and related security risks; confidential access control; communication trends and patterns in the use of massive communication strategies; intellectual property and product risk management; resource management; financial considerations and accountability; and safety. Several technologies and personal practices are reviewed, as well as ways to mitigate or eliminate their associated risks. The core principles of information security - confidentiality, integrity, and availability - provide an overall framework.

Keywords: Information Security, Privacy, Risks, Security, Social Media, Virtual Worlds

INTRODUCTION

Virtual worlds and social media impact a wide range of activities including E-Commerce, business communication, and marketing. People have adapted virtual personas in social media sites such as Facebook, Instagram, and Pinterest at a rapid rate. Corporations and organizations have also been aggressive in leveraging social media to further their goals. Not all uses have been for positive activities as virtual worlds and social media have become a commonly used tool by terrorists to plan, execute, and even display terrorist activities (Rosenblatt, 2013). A major challenge is that virtual worlds provide an incredible amount of information and opportunity to potentially exploit businesses and individuals. Crimes such as identity theft, fraud and virtual stalking are becoming so prevalent and damaging that the current incarnation of the Internet may become an insurmountable threat if security and privacy concerns are not aggressively and adequately addressed. The use of virtual worlds and social media by terrorist organizations and organized crime raise issues such as whose responsibility it is to curtail such activities, something that is further complicated by the imprecise laws, regulations, and enforcement in the global environment. In reaction to this use, law enforcement agencies and...
organizations such as the National Security Agency use and monitor virtual worlds and social media.

This investigation will analyze the use and capabilities of current and emerging virtual technologies including social media, gaming, blogs, virtual meetings and virtual worlds in the context of their productive utility and security risks presented. Security and privacy concerns will be investigated in the following areas:

1. Exploits, Vulnerabilities, and Related Security Risks
2. Confidential Access Control
3. Communication trends and patterns in the use of massive communication strategies
5. Resource Management
6. Financial Considerations and Accountability
7. Safety

The investigation will conclude with a summary and a look at emerging trends and future direction in security and privacy of virtual worlds, social media, and E-Commerce.

Context

In the late 1990’s, E-Commerce was hyped as a way for small start-up companies to compete on a level playing field with established corporate behemoths. The demise of brick and mortar stores was widely predicted and common sense business practices were thought of as outdated. The “Internet Bubble” burst by 2001 and most realized the error in forgetting the basics. Companies learned a lot about the Internet, E-Commerce and their business during the Bubble, but an area that lagged the Bubble in terms of attention and focus was that of security. Ten years later, hacking, identity theft, privacy and similar information security issues have become central to the business model.

Social networking through the use of Internet sites such as Facebook, YouTube, LinkedIn, Twitter, and Pinterest are among the most popular uses of the Internet in 2013, with Facebook #2, YouTube #3, LinkedIn #8, Twitter #10 and Pinterest #26 in Alexa’s rankings of the top 500 global Internet sites (Alexa.com, 2013). Online gaming and virtual world technology have become mainstream, aided by the advancement of home gaming systems gaining Internet technology. This has led to massively multiplayer online role-playing games (MMORPG), which can entail literally tens of thousands of players participating in an online gaming experience in a virtual world.

Virtual worlds like Second Life, There.com, and more business-focused offerings are on the brink of becoming valuable work tools. Major companies and public-sector organizations — such as BP, IBM, Intel, and the United States Army — are investing heavily in virtual world technologies (Driver & Jackson, 2008). In fact, Driver and Jackson predict that by 2013 the 3-D Internet will be as important for work as the Web in its current form. This view was supported in an article in CIO magazine (Lynch, 2008) that projected enterprise versions of online virtual worlds like Second Life would be just as important to business as the Web is today. This may be a stretch because the same research organization (Forrester Research) recently reported that “only 11% of enterprises have adopted virtual worlds to augment their work.” (Rutherford, 2009).

From the point of view of most business leaders, the utility of virtual worlds in business is not apparent. Keitt (2009) attributes this to virtual world vendors not doing a particularly good job articulating their value. Instead, the central message of virtual world providers is that they allow for groupings that can be augmented or reduced on the fly while also allowing users to consider information from multiple applications simultaneously. King (2008) reports that companies such as IBM, Sun, Xerox, Cisco and Unilever are using 3D technology and virtual worlds in this very manner for things like strategy sessions, employee meetings, mixers, and recruiting. While the use of virtual worlds for functions such as E-commerce shows much promise, security and privacy are critical success