

“The New and Virtual Wild, Wild West”

Protecting our Digital Identities in Cyberspace

by Deborah Taylor Tate

(Prepared for delivery at Telecom World 2009, October 6, 2009 in Geneva Switzerland)

Thank you for joining this esteemed panel of global experts who will assist us not only in providing some information regarding some of the most novel and incredible opportunities technology is providing today---from positively impacting the world economy to improved healthcare to civil participatory involvement and even online voting-- but also the challenges of protecting our corporate, customer, employee and consumer digital identity in this “Wild Wild West” of the digital age.

Cybersecurity is no longer merely a threat for corporations or government, but presents very real risks to all of us—individuals, small and large enterprise, families and children; every time we log on. And, we will also hear from this panel regarding the use technology to combat and more importantly, to prevent these risks including security solutions such as authentication and malware detection tools. However, we must also recognize and encourage the education of individual users at every level; and to encourage personal, corporate and government responsibility to protect personal and private information found within our digital footprints.

What the Information Age has changed about theft, is the speed and method by which identity thieves can access and exploit the personal information of others. One method in particular leaves hundreds of thousands, and in some cases tens of millions, of individuals at risk for identity theft: large scale data breaches by skilled hackers. Criminals are able to remotely access the computer systems of government, universities, business, financial institutions, credit card companies, and data processors, and steal large volumes of personal information in one fell swoop. Such large scale data breaches have revolutionized the identity theft landscape as it relates to fraud on existing accounts through the use of compromised credit and debit card account information.

Large scale data breaches would be of no more concern to law enforcement than small scale identity thefts except for this new viral nature that allows the immediate and virtual distribute of the stolen information for even additional

fraudulent purposes. Compounding this speed of distribution is also the unknown amount of time for detection of the original breach. According to the U.S. Department of Justice, this wide-scale global distribution of stolen information is possible through the advent of criminal websites, known as “carding forums.” These websites are global businesses dedicated to the sale of stolen of our personal and financial information. These websites allow criminals to immediately sell the loot from ill-gotten gains to interested buyers globally.

And we will all must learn an entirely new vocabulary: Trojan horses, multi-purpose bots, spyware, ward-driving, sniffing, phishing and pharming. Phishing and pharming are two of the most popular forms of fraud that dupe innocent victims into falsely believing they are a trusted Web site such as their own bank, when in fact they have been enticed to a bogus Web site which then steals their identity and possibly drains their finances. The trillion dollar price tag of this crimewave is often based on the heightened sensitivity of data such as bank and credit card information while often remaining undetected by the victim.

Almost daily we read of a serious security or information breach:

*U.S. Government employee who misplaced laptops with thousands of American citizens personal data and social security number;

*Healthcare information being faxed over and over to the wrong medical facility with extremely sensitive data and more problematic—delaying medical treatment and payment to the appropriate provider;

*Financial institutions facing today’s “Bonnie and Clyde” online

*Security breaches by major retailers with the potential impact to literally millions of consumers worldwide

Mobility: Asset and Challenge

And these examples are only multiplied by the challenges of our increasingly mobile world—notebooks, laptops, hand-held devices are not just for road warriors any more. Wireless has become not only a cost-saving measure but a strategic corporate asset across the enterprise and increasingly government sector as well.

These technologies provide us with good news including increasingly higher productivity of the workforce. This becomes more important as our workforce is also working differently as telecommuters are increasing and projected by 2015 to

be greater than mass transit commuters. Finally, in these days of the H1N1 Flu, and looming concerns of a potential pandemic or other natural disaster which could preclude workers from working outside the home, mobile security needs beyond the corporate setting become paramount. This becomes even more crucial in global, national and corporate disaster planning; and also may lead to increased need for investment in infrastructure in residential areas which may become the workforce headquarters in times of disaster.

Mobility, it is clear, is an all-around winning strategy that merits a larger role as a strategic asset. Overall IT costs are reduced and companies can even improve their environmental footprint. However, laptops and notebooks—not to mention handheld devices—are seldom if ever “bolted down” and will likely be taken off campus, so the threat of theft is much greater. In addition, wireless devices are likely storing sensitive data and are configured with protocols to gain access into the entire corporate network from anywhere, utilizing many access points, numerous networks and a web of varied technologies.

Thus, corporate security policies must ensure workers are able to achieve maximum benefit—safely, responsibly, remotely and swiftly. To support this rapidly evolving environment, IT must leverage next-generation remote management and anti-theft tools—to broaden remote access, provide collaboration tools, and securely manage mobile assets; employing up to date technology, which provides all devices with hardware-based security and enhanced maintenance, oversight and management capabilities which you will hear more about from our panel.

Children and Cybersecurity

Just as we are dealing with cyber-threats to governments, corporate secrets, financial institutions, scientific discoveries and artistic content; we must also include our children and youth in this ecosystem. Their use of technology is incredible and baffling. Multi-tasking is no longer unique; it is the norm. One study says our children consume 8 hours of media in 6 hours. “Screentime” includes multiple devices and technologies, consuming over 45 hours of media per week. Children now make up over 19% of Chinese “netizens” and are a \$3 (three) billion dollar sector for U.S. advertisers. And as global deployment increases, so will the numbers of children online. In many developing nations, children and youth are the early adopters; they will see both the benefits and the risks first—often before parents and caregivers may even realize the pitfalls.

A recent U.S. study also showed that while our youth are improving their academic performance, creating and sharing their own creative works online; they are also utilizing technology for cheating in school and even hacking into another teen's account and stealing their identity to communicate with others. Just as in the offline world, we must teach our children and youth digital literacy and knowing "right" from "wrong" online.

With Cell phones marketed to preschoolers and children going online at earlier and earlier ages (3-5 for present college students). In both developed and developing nations a child's only connection may be a mobile device which can in many cases link them directly to the internet, the world and of course criminal, rogue and deviant behavior.

So, for you who represent both corporate and Government, for you who are parents and educators, please remember whether through policy, regulation, curriculum or product design, we must be cognizant of our children—not as an after-thought—but as we are watching these cybersecurity issues unfold.

In fact, the youth of the world will be the consumer drivers of new technology and you should be watching closely their behavior, uses, purchasing power----because technology will allow them to access incredible opportunities of education, healthcare and the jobs of tomorrow. Hence, we want to insure not only that their digital footprint, personal and financial data will be safe but also that they will become good global digital citizens—"Good Digi-zens"—wherever, whenever and however they connect.

To that end, I hope you all will visit the ITU's "Child Online Protection Initiative- or COP" at www.itu.int/cop which is a global repository of tools and educational materials for your review and use. Whether you are a public official or parent; a corporate provider or caregiver; teacher or student—we hope you will find information and tools and research so that together we can all help insure that our children are connected—safely and responsibly. The online opportunities are limitless for bridging the digital divide and allowing all our children to reach their full potential. For they are indeed the global leaders of tomorrow.