

IT Security & Authentication: Key Concerns for 2010

Information Technology Professionals Survey

Based on a recent survey of IT professionals, this report examines the top security issues IT professionals and their companies should be prepared to address in 2010.



PhoneFactor, Inc.
7301 West 129th Street
Overland Park, KS 66213
1-877-No-Token / 1-877-668-6536
www.phonefactor.com

IT Security & Authentication: Key Concerns for 2010

With the growing number of data security breaches and the increasing sophistication of the attacks and the attackers, IT security is top of mind for both businesses and consumers. The survey discussed in this paper investigated the opinions and attitudes of IT security professionals on the state of IT security in their workplace and in their personal life. It also delved into the role of and confidence in current user authentication practices. The survey is a follow-up to one conducted the previous year and demonstrates historical trends as well as emerging thoughts on IT security.

This year's survey analyzed 265 responses, up from 204 the previous year. All participants held an IT security job function within various industries; company size and title varied. Participants were emailed an invitation that included a brief overview of the survey goals, and asked to spend a few minutes of their time to complete it. The results were then compared to the previous year's, as well as analyzed for specific data points within just that year's survey.

Contents

Increased Threats & Fiscal Accountability Define IT Security Today	3
Concern Is Growing - Current IT Security Practices Just Aren't Enough	3
<i>Image 1: Corporate Priority Level for Security</i>	4
Mitigating Risk Is Clearly Assigned as a Corporate Responsibility	4
<i>Image 2: Corporate Data or Network Ever Compromised</i>	5
<i>Image 3: Businesses Responsibility for Protecting Your Personal Data</i>	5
The Reality of the New Threat Environment	6
<i>Image 4: Greatest Corporate IT Security Threat in the Next 12 Months</i>	6
Confidence and Satisfaction Are Dropping - A New Methodology Is Needed	7
<i>Image 5: Perception of Company's Current Authentication System(s)</i>	7
<i>Image 6: Barriers to Adopting Strong Authentication</i>	8
<i>Image 7: Satisfaction Level of Current Method for Securing User Access</i>	8
<i>Image 8: Users' Preferred Security Device</i>	9
Two-Factor with a Cell Phone Provides the Best Solution	9

Increased Threats & Fiscal Accountability Define IT Security Today

2009 was been a tough year for those in IT security roles. Threats continue to increase in both sophistication and frequency, and many of the safeguards in place don't offer adequate protection. The victims of these attacks (both companies and individuals) are paying a high price. For instance, according to Heartland Payment Systems CEO Robert Carr, they paid more than \$32 million in the first half of 2009 alone in response to the largest data security breach to date (CSO, October 2009).

Heartland was PCI DSS compliant and had passed a recent audit, so most believed their data security to be sufficient. But PCI DSS has become greatly contested, with many asserting that it is just a baseline and corporate security policies should be much more stringent. In fact, courts are beginning to support this theory. As of this writing, Heartland is in the middle of a class action lawsuit. And they are not alone.

The banking industry is also starting to experience legal ramifications. Western Beaver School District is suing ESB Bank for malware that drained \$700,000 out of their account (The Washington Post). Slack Auto Parts had malware on their controller's PC that allowed attackers to set up dummy accounts and transfer \$75,000 (New York Times). Bullitt County, Kentucky, wire transferred \$415,000 to mule accounts as a result of malware on the county treasurer's PC (The Washington Post). Similar to Heartland's situation, all banks in question were FFIEC compliant.

Finally, Citizens Financial Bank is being sued by a couple for fraudulent activity on their account in the amount of \$26,000 – they claim the bank didn't utilize strong authentication and the court ruled against a motion to dismiss, so it is heading to trial (BankInfoSecurity.com).

Concern Is Growing – Current IT Security Practices Just Aren't Enough

The bottom line is that consumers are holding organizations responsible for protecting their data. It's no surprise then that nearly two-thirds of companies ranked IT security as a "high" priority, a 15.56% increase over the 2008 survey.

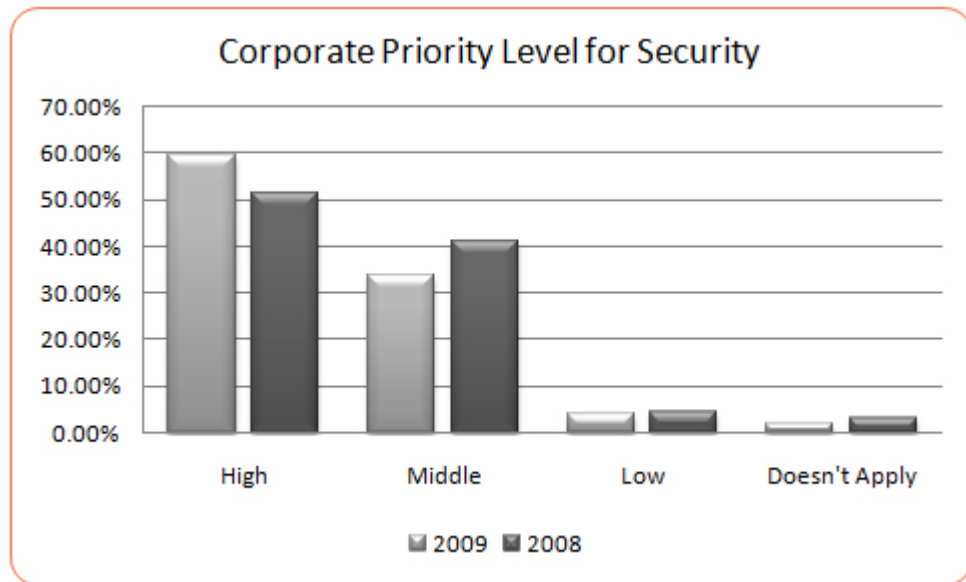


Image 1: Corporate Priority Level for Security

Additionally, the majority of respondents acknowledged that a simple user name and password are just not adequate protection for either employee or customer access. Nearly three-quarters (72.08%) indicated this combination was insufficient for employee access, while a slightly lesser amount (67.55%) found that it was insufficient for securing customer access.

While a majority of respondents (69.81%) feel that employee and customer access are both equally vulnerable to attack, they were slightly more concerned about securing employee access. Of respondents, 80.38% were either extremely or moderately concerned, compared to 76.22% reporting the same level of concern about securing customer access. However, the preponderance of concern about protecting both pathways is apparent.

Mitigating Risk Is Clearly Assigned as a Corporate Responsibility

This growing concern is likely coming from the personal impact of 2009's increased threat environment. Both corporate data breaches and incidents of personal identity theft are on the rise. One in four respondents reported that their company's network or data had been compromised, up from one in five the previous year. And, nearly one in three respondents has experienced identity theft or fraud personally, also up from one in five the previous year.

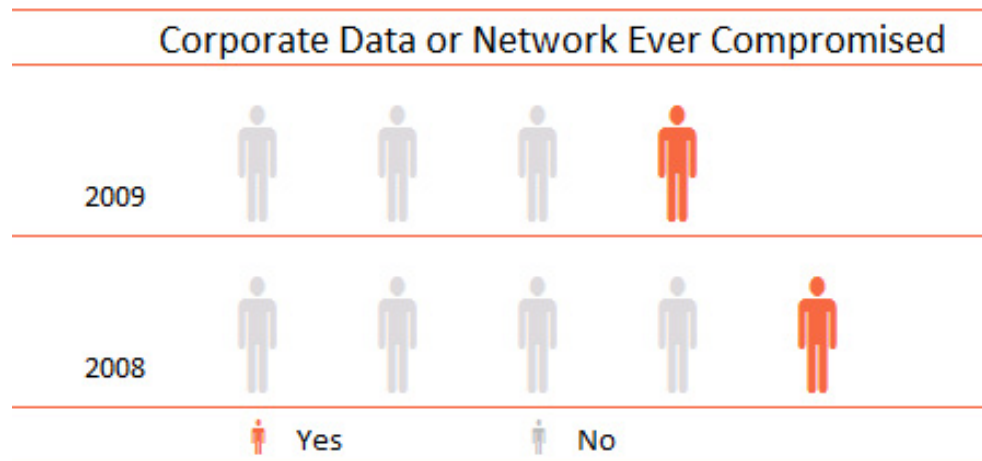


Image 2: Corporate Data or Network Ever Compromised

Respondents appear to be primarily concerned about the emotional impacts of identity theft and fraud, reporting unknown issues that could be damaging to them and loss of personal control over their vital information as their biggest concerns.

They are squarely placing responsibility for protecting both corporate and personal data on the organizations with whom they entrust their information. More than three-fourths (77.06%) of respondents feel that businesses to which they give their personal or financial data as a consumer are either extremely responsible or very responsible for protecting their personal or financial information. This includes a whopping 51.5% who reported that businesses are extremely responsible for protecting their personal information.



Image 3: Businesses Responsibility for Protecting Your Personal Data

The Reality of the New Threat Environment

Poor password practices are clearly an issue with IT security personnel, with 27.67% of respondents reporting it as the greatest external threat to their company's IT security in the next twelve months. However, malware is the greatest perceived threat (49.01% of respondents). Nearly one-third of respondents (32.41%) felt that malware installed on PCs posed the greatest external threat and an additional 16.60% indicated that malware on mobile devices presented the greatest external threat.

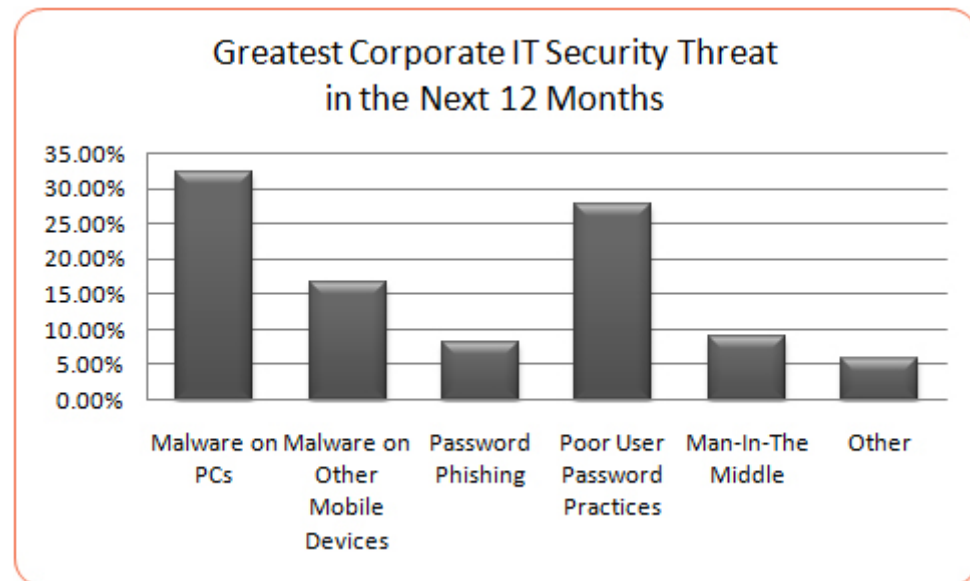


Image 4: Greatest Corporate IT Security Threat in the Next 12 Months

Malware has plagued online banking recently with the proliferation of banking trojans like Clampi and ZeuS among others. The Clampi trojan alone is reported to have infected more than 500,000 computers since March of 2009. The trojan sits in wait for a user to access one of more than 4,600 online banking, government, and business services websites then initiates fraudulent wire transfers. This particular trojan is targeting businesses, not consumers, in hopes of gaining access to higher balance accounts. And it circumvents security tokens and one-time password technologies designed to protect online banking users.

For enterprises with increasingly mobile workforces and a growing number of mobile devices to protect, concern about the threats posed by these new types of attacks is a fierce reality to face when partnered with a lacking password standard.

Confidence and Satisfaction Are Dropping— A New Methodology Is Needed

In contrast to the level of responsibility respondents placed with corporate entities, confidence in corporate authentication policies securing data is poor and rapidly dropping. Only 35% of respondents feel that their company's current authentication system is either very or extremely secure, down 16.62% from the previous year. And, those that feel that their system is not at all secure have increased by more than 66%. Finally, more than 20% rate the security of their current system as not at all or only somewhat secure.

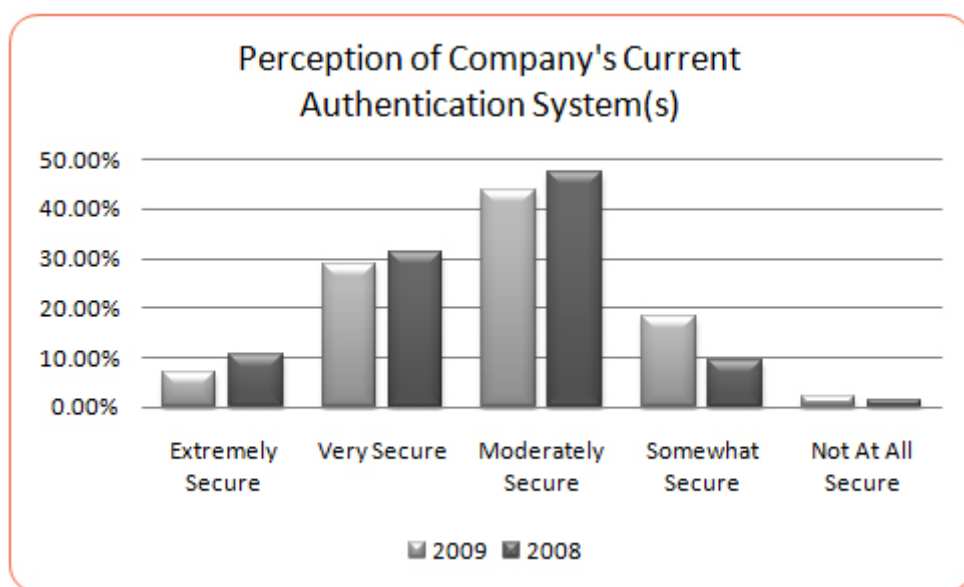


Image 5: Perception of Company's Current Authentication Systems

The reason for adopting strong authentication is clear; companies must do everything they can to protect themselves. As evidenced by the many pending lawsuits mentioned earlier, mere compliance is not enough. In fact, only 21.13% of respondents listed regulatory compliance as the overriding reason for adopting two-factor. The overwhelming reason for implementing two-factor for most respondents was to prevent a security breach (58.87%).

However, there are many barriers to implementing or upgrading a two-factor authentication system, and these have remained constant over the past few years. The largest barrier to adopting stronger authentication continues to be cost (34.42%). This is closely followed by the time to deploy and manage two-factor (25.96%), and user inconvenience (25.77%).

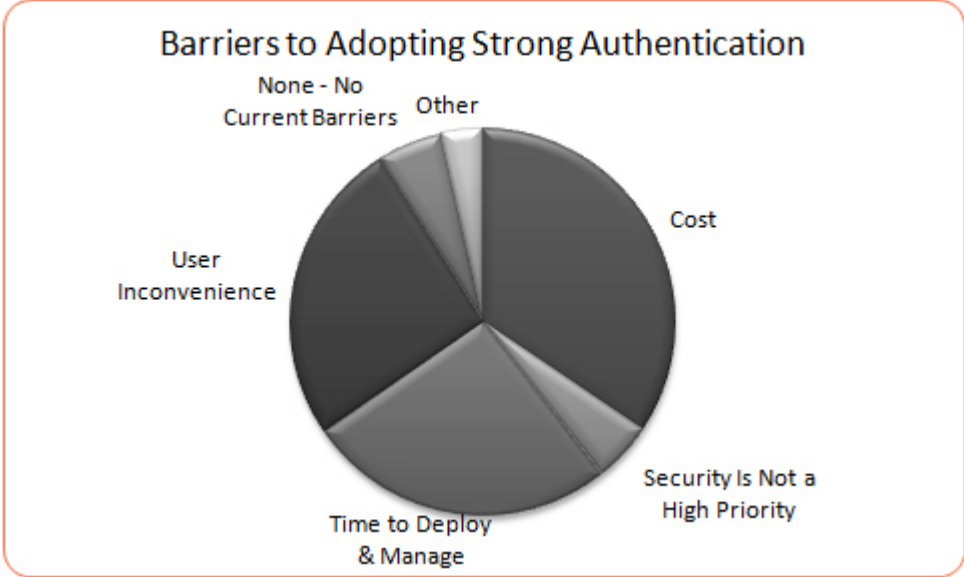


Image 6: Barriers to Adopting Strong Authentication

Unfortunately, most respondents are only moderately or less satisfied with their current method of securing access (73.59%), and they believe the same to be true for their users (66.54%). In fact, nearly 8% of IT professionals surveyed are not at all satisfied with their current method of securing user access.

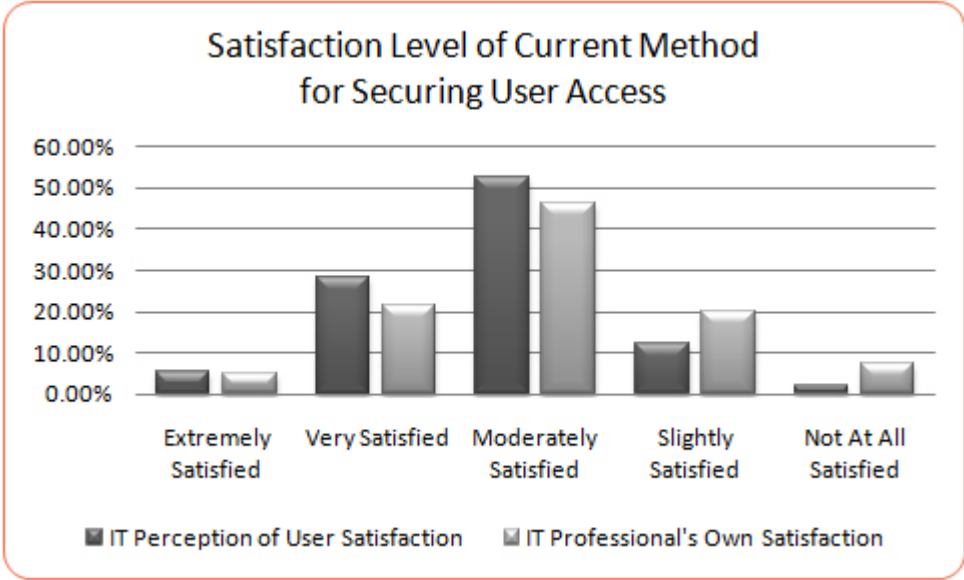


Image 7: Satisfaction Level of Current Method for Securing User Access

The bulk of respondents (57.36%) believe that their users would prefer to carry a cell phone over other two-factor authentication devices such as a security token or fob, a USB token or fob, a grid card, or a smart card. The cell phone option actually scored better than all others combined, with the nearest other option

reporting at only 15.47% of respondents. In fact, 70.31% of respondents agree with Wired Magazine's claim that security tokens are a "top 10 worst gadget ever."

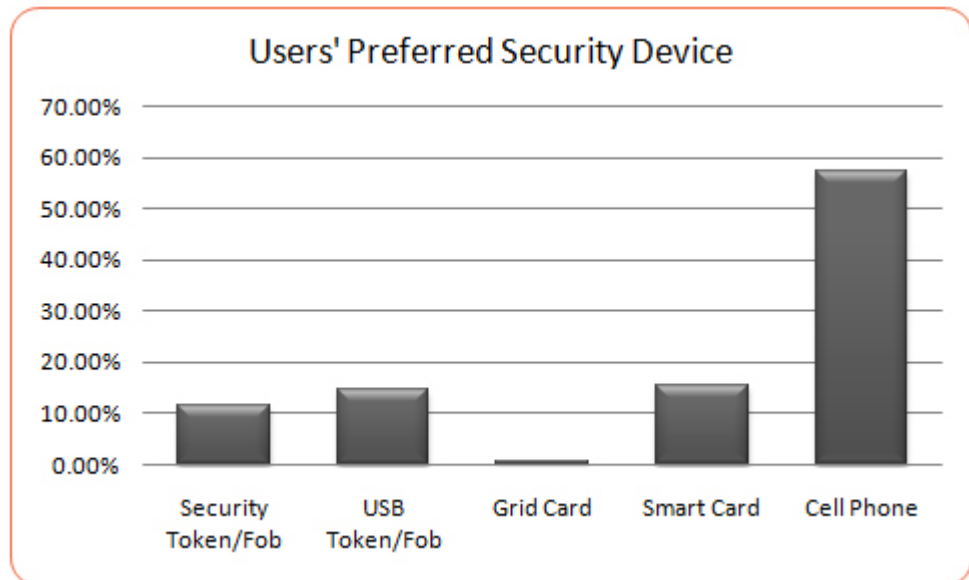


Image 8: Users' Preferred Security Device

Two-Factor with a Cell Phone Provides the Best Solution

While the need for two-factor authentication is clear, some forms of two-factor may not be enough to truly protect against a catastrophic security breach, both as employees and consumers. Specifically, not everything defined as two-factor truly is that, and out-of-band security is a must to protect against the most menacing threats.

IT professionals have a unique perspective since they have a stake in the game as both a user and a security expert. They know that a successful two-factor implementation must be cost-effective (both initially and ongoing), user-friendly, and secure. They have indicated that users would prefer to use a cell phone as their security device. Doing so with PhoneFactor breaks down all of the typical barriers to implementing or upgrading a two-factor system.

- **It's easy for users** – They carry their cell phone with them all the time. All they have to do is press # (or enter a pin) when they are asked to authenticate.
- **It's cost effective** – There is no additional equipment to buy, and nothing to install or maintain on user equipment. There are no devices to distribute, and training and support are minimal. Initial costs are significantly lower than other solutions, and ongoing costs are nominal.

- **It's more secure** – PhoneFactor's out-of-band technology uses a completely separate channel to authenticate the login, so even if your computer or network is hijacked, the phone line remains secure. Add to that transaction verification and real-time fraud alerts, and PhoneFactor is the offers unparalleled protect against today's most sophisticated threats.

For more information on PhoneFactor, please visit www.phonefactor.com.