



# Data Security: Social Networking and the New Human Security Perimeter

## POWERFUL INSIGHTS

---

### Issue

Since the early days of its development, the Internet has been leveraged as a social platform, and people continue to meet, connect, organize, share and collaborate online in unprecedented fashion. We live in the information age, where a knowledge-based economy demands that workers have access to relevant channels to both foster communication and facilitate collaboration on projects. Thus, it is only natural that web-based social networking applications have begun to creep into the business environment.

### Challenges and Opportunities

While many companies have yet to embrace social networking, more and more organizations see it as an enabler for business operations and, similar to other communication mediums (such as e-mail), treat access to such sites by applying the appropriate practices and technology to reduce their risks.

While opening access in the workplace to these social networks can create numerous long-term benefits, there are risks involved, including reduced employee productivity and, perhaps more notably, information security breaches. Key security risks include:

- Potential data leakage of sensitive information
- Unintentional upload of Trojans or viruses to employee computers
- Increased targeting of individuals who are associated with your company for social engineering attacks
- Individuals falling prey to fraudulent scams

The most prominent threats are either technical or social in nature. Technical breaches primarily occur through web application security weaknesses or poor practices by employees uploading or downloading inappropriate content. Social threats relate mainly to social engineering attacks or malicious users gaining information from unsuspecting employees.

A recent industry poll found that 30 percent of companies experience a security incident as a result of employee activities on an Internet social networking site. Employees increasingly are targeted by social engineering attacks whereby an individual will use personal manipulation, deception and/or influence to obtain sensitive information. This, in turn, enables a more technologically based attack on the network or data.

### Our Point of View

The responsibility for security needs to shift from a technology-based focus to the people who comprise an organization. After all, people, through their actions and behaviors, have the most significant role in securing the enterprise. By building a strong communication program and heightening the overall risk consciousness, organizations can help their employees recognize risky behavior and respond to attacks, thus creating a human security perimeter.

Most organizations are either evaluating or have implemented formalized policies regarding employee participation in social networking sites. Policies should include guidelines on what information can be discussed through these mediums and how to treat content obtained or downloaded from these sites. Policies also should reinforce the message that Internet access is provided for business purposes and should not be abused, thereby permitting disciplinary action if productivity concerns are raised.

Once the development of standards and practices is complete, companies must turn to educating their employees. Employee education and awareness, in tandem with strong technical security controls such as anti-virus, anti-spyware and web filtering technology, will help clarify how to use technology to achieve the expected results while also reducing the likelihood that these risks will impact your business. ➤

## PROVEN DELIVERY

### How We Help Companies Succeed

Protiviti's security and privacy team understands the inherent risks our clients face in embracing new technology. Using a combination of skills drawn from information security, data privacy, technology, internal audit, risk, regulatory compliance, communications and marketing, we assist clients in addressing their data security needs in a holistic manner that is easy to understand, pragmatic and in-line with industry best practices.

A key driver of this approach is the internal communication and training group of Protiviti. As a full-service agency, we have worked with companies around the world to address their employee communication challenges and introduce a behavioral approach to change management across an array of mediums, including:

- Print and interactive awareness campaigns that bring policies and strategies to life
- Interactive training and in-class support material that engages employees and ensures they understand their roles, responsibilities and accountabilities
- Web portals that track the results of a training effort and facilitate communication across the enterprise

For more information or to contact one of our communication experts, please visit [www.protiviti.com](http://www.protiviti.com).

### Contacts

Pat Quinn  
+1.519.746.6644  
[pat.quinn@protiviti.com](mailto:pat.quinn@protiviti.com)

Rocco Grillo  
+1.212.603.8381  
[rocco.grillo@protiviti.com](mailto:rocco.grillo@protiviti.com)

Ryan Rubin (London)  
+44.207.389.0436  
[ryan.rubin@protiviti.co.uk](mailto:ryan.rubin@protiviti.co.uk)

### About Protiviti

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

### Example

A global consulting firm wanted to communicate the sensitivity of data losses and foster an employee culture that emphasized data security. To achieve these objectives, a two-pronged approach was developed.

A broad review of the organization's security policies led to revisions to the current protocols and a rollout of laptop encryption software to all consultants. Once the policies were in place, our team partnered with management to utilize a blended learning approach that included print awareness, online interactive and face-to-face training to emphasize the consequences and costs of data theft to the company and its reputation. The campaign featured a launch e-mail, posters, face-to-face presentation material and an online interactive training module to provide an in-depth look at data security. The print material was developed in English and translated into Korean and Japanese.

Employee feedback and audit findings at our client indicate increased awareness of laptop and data security and heightened compliance with policies and procedures. Furthermore, there have been no noteworthy incidents of data theft. Given that the estimated cost of losing a laptop computer containing proprietary client information is more than \$50,000, the client has seen a significant return on its investment.