THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY:
A SURVEY OF IT PROFESSIONALS

Dimensional Research | September 2011

Introduction

The threat of technology-based security attacks is well understood, and IT organizations have tools and processes in place to manage this risk to sensitive corporate data. However, social engineering attacks are more challenging to manage since they depend on human behavior and involve taking advantage of vulnerable employees. Businesses today must utilize a combination of technology solutions and user awareness to help protect corporate information.

The following report, sponsored by Check Point, is based on a global survey of 853 IT professionals conducted in the United States, United Kingdom, Canada, Australia, New Zealand, and Germany during July and August 2011. The goal of the survey was to gather data about the perceptions of social engineering attacks and their impact on businesses.

Key Findings

- **The threat of social engineering is real**
  - 97% of security professionals and 86% of all IT professionals are aware or highly aware of this potential security threat
  - 43% know they have been targeted by social engineering schemes
  - Only 16% were confident they had not been targeted by social engineering, while 41% were not aware if they had been attacked or not
- **Financial gains are the primary motivation of social engineering**
  - 51% of social engineering attacks are motivated by financial gain
  - 14% of social engineering attacks are motivated by revenge
- **Social engineering attacks are costly especially in large organizations**
  - 48% of large companies and 32% of companies of all sizes have experienced 25 or more social engineering attacks in the past two years
  - 48% of all participants cite an average per incident cost of over $25,000
  - 30% of large companies cite a per incident cost of over $100,000
- **New employees are most susceptible to social engineering techniques**
  - New employees (60%), contractors (44%), and executive assistants (38%) are cited to be at high risk for social engineering techniques.
- **Lack of proactive training to prevent social engineering attacks**
  - Only 26% of respondents do ongoing training
  - 34% do not currently make any attempt to educate employees, although 19% have plans to

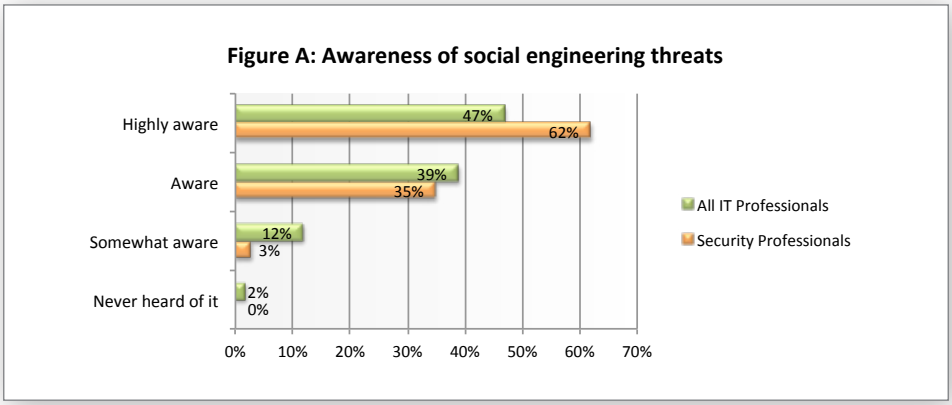
dimensional research

Sponsored by Check Point SOFTWARE TECHNOLOGIES LTD.

Detailed Findings

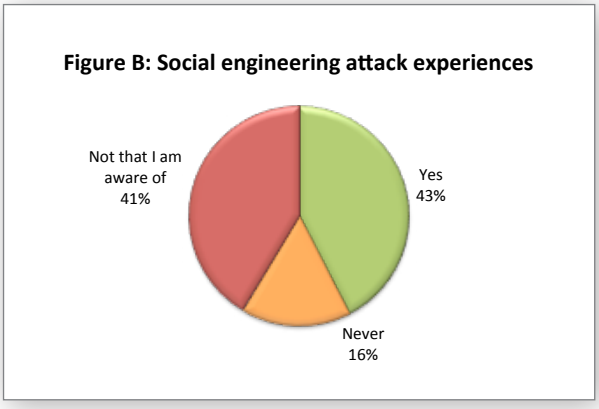
Awareness of social engineering high among IT professionals

Participants were asked to rate their level of awareness of the potential security threat of social engineering attacks. In general, IT professionals reported a high degree of awareness (86%) — 39% described themselves as aware and 47% highly aware. And among security professionals whose entire job was to secure their organizations systems, awareness was even higher (97%) — 35% were aware and 62% highly aware. See **Figure A**.



Many businesses have already faced social engineering attacks

Participants were asked if their organizations have been targeted by social engineering attacks. While 43% of participants indicated that they had, only 16% had confidence that they had not been targeted. A large number of participants (41%) were not aware of any attacks, but could not say definitively that there had not been an attempt. This response implies a potential risk that businesses and IT teams are not dealing with. See **Figure B**.



What is Social Engineering?

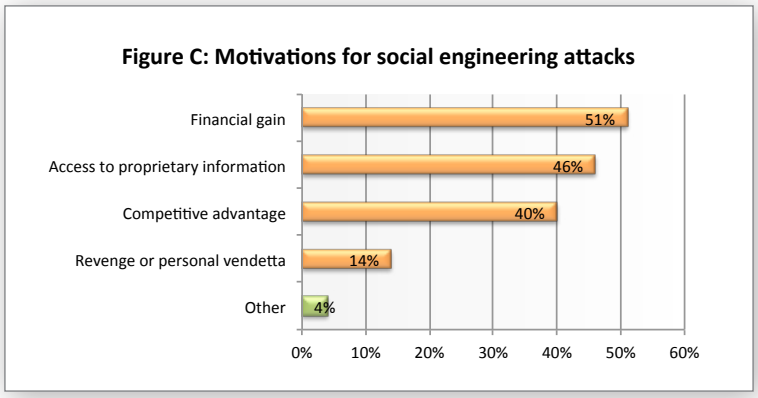
Participants were given this definition of social engineering before answering the survey questions:

Social Engineering is the act of breaking corporate security by manipulating employees into divulging confidential information. It uses psychological tricks to gain trust, rather than technical cracking techniques. **Social Engineering** includes scams such as obtaining a password by pretending to be an employee, leveraging social media to identify new employees more easily tricked into providing customer information, and any other attempt to breach security by gaining trust.

The highest rate of social engineering attacks (61%) was reported by participants who work in energy and utilities. Nonprofits experienced the lowest level of social engineering attacks (24%).

Social engineering attacks motivated primarily by financial gain

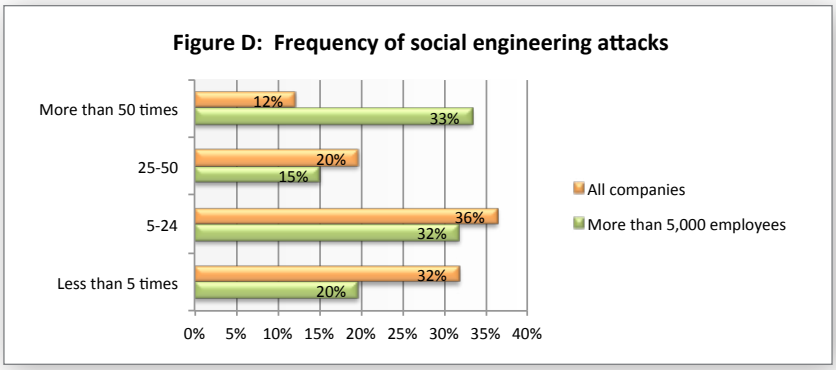
The participants who indicated that they had been victims of social engineering attacks were asked what they believed the motivations were behind those attacks. Financial gain was cited as the most frequent reason (51%), followed by access to proprietary information (46%), and competitive advantage (40%). Fortunately, revenge was the least likely reason for a social engineering attack with only 14% reporting this as a motivator. See **Figure C**.



Motivations for social engineering attacks varied slightly in different countries. Australians (61%) and Americans (52%) were the most likely to cite financial gain as a motivation. Germans reported more revenge-motivated attacks (18%), while Canadians were more likely to experience attacks motivated by competitive advantage (54%).

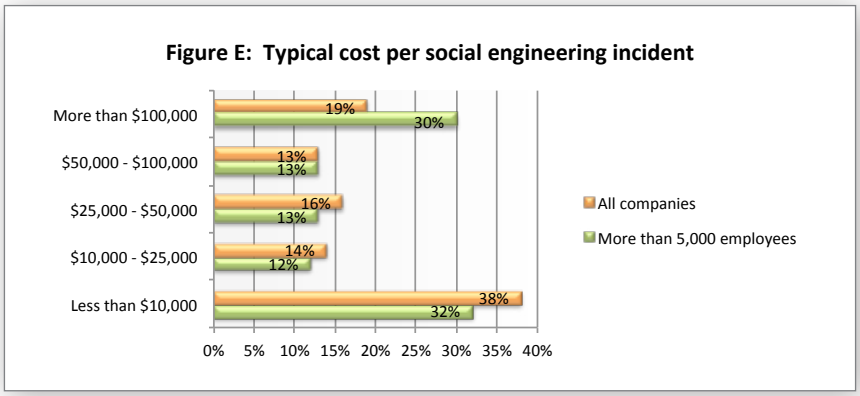
Social engineering attacks happen frequently

Participants who had been targeted by social engineering attacks and also tracked these incidences were asked about their frequency (N=322). Social engineering attacks were a frequent occurrence with 32% of all participants reporting 25 or more attacks during the past two years. Unsurprisingly, larger organizations were attacked even more frequently with 48% of participants reporting 25 or more attacks in the past two years. See **Figure D**.



Social engineering attacks are costly

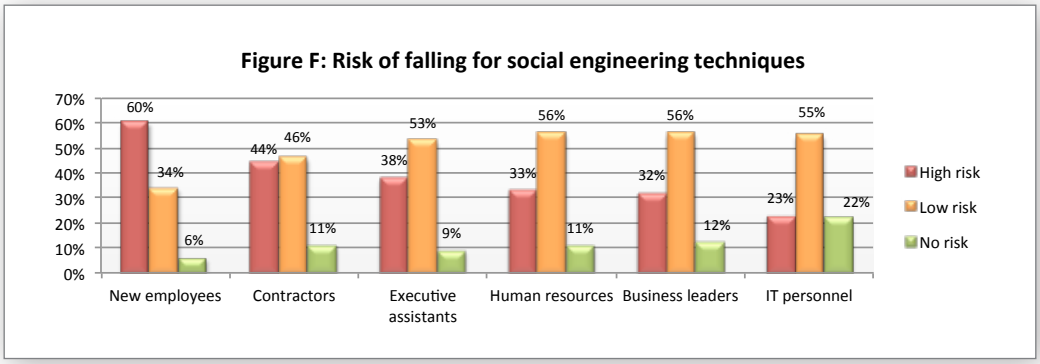
Participants who had been targeted by social engineering attacks and tracked these incidences were also asked about the typical cost of each incident (N=322). Costs included business disruptions, customer outlays, revenue loss, labor, and other overhead. These attacks were frequently costly with almost half of participants (48%) reporting a per-incident cost of more than $25,000. Again, larger organizations reported even higher costs with 30% reporting a per-incident cost of more than $100,000. See **Figure E**.



Across industries, financial services and manufacturing reported the highest average per-incident cost, and educational institutions and non-profits reported the lowest costs.

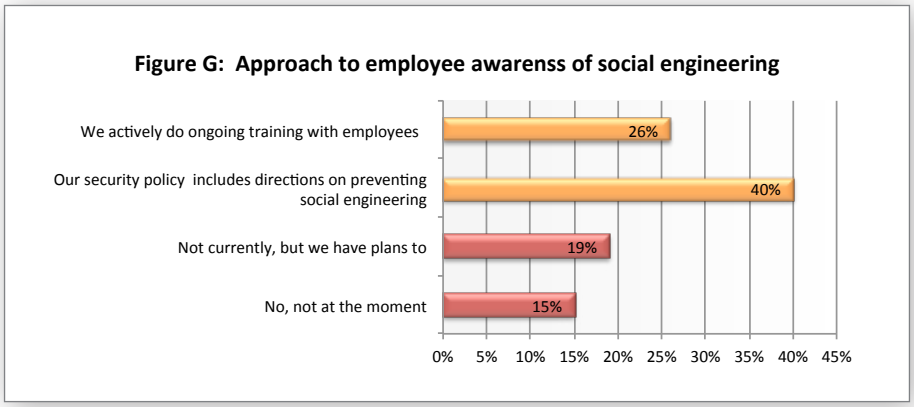
New employees present greatest risk for social engineering attacks

All participants were asked what type of personnel was the most likely to be susceptible to social engineering techniques. New employees were considered the highest risk (60%), followed by contractors (44%) who may be less familiar with corporate security policies, and executive assistants (38%) who have access to executive calendars and confidential information. See **Figure F**.



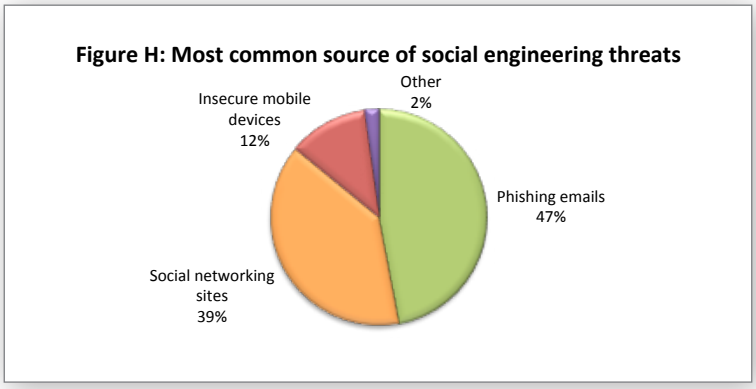
Few companies proactively train on risk of social engineering

All participants were asked what their organization was doing to prevent social engineering attacks. Only 26% of participants actively train employees on the threat. An additional 34% do not have any initiatives in place now, although some of those (19%) do have plans to start a program to educate employees. The largest segment of participants, 40%, put the responsibility on the employee to read and understand their organization's overall security policy documents to prevent data loss, security attacks, and social engineering-based threats. See **Figure G**.



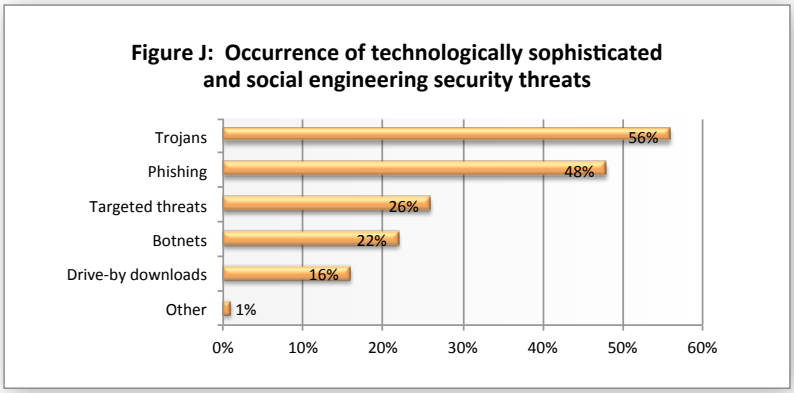
Phishing emails most common source of social engineering

Participants were asked their opinion on the most common source of social engineering threats. Phishing — pretending to be a trustworthy entity in an electronic communication — was identified as the most typical source (47%), followed by social networking sites such as LinkedIn that allow new employees to be targeted (39%). See **Figure H**.



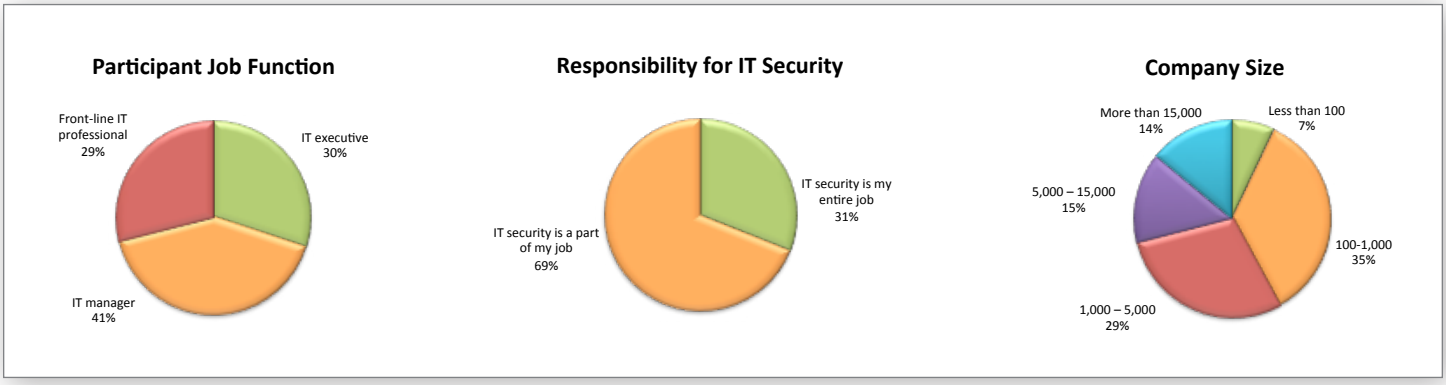
Sophisticated technology-based security threats continue

Organizations across all sizes and industries have experienced a variety of both technologically sophisticated and social engineering attacks, indicating a clear need to manage both technological and social engineering attacks. Participants reported that they were most likely to experience trojans (56%), followed by phishing techniques, botnets, and drive-by downloads. See **Figure J**.



Survey Methodology

In July 2011, an independent database of IT professionals was invited to participate in a Web survey on the topic of social engineering and information security sponsored by Check Point. A total of 853 respondents across the U.S., UK, Canada, Australia, New Zealand, and Germany completed the survey, all of whom had responsibility for securing company systems. Participants included IT executives, IT managers, and hands-on IT professionals and represented a wide range of company size and industry verticals.



About Dimensional Research

Dimensional Research® provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information visit www.dimensionalresearch.com.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.