



## COMUNICAT DE PRESĂ

### Un studiu global relevă o percepție surprinzătoare asupra rolului profesioniștilor IT în securizarea informațiilor companiilor

*În pofida comportamentului online riscant, tot mai mulți lucrători la distanță consideră că managerii – nu personalul IT – au dreptul să controleze activitățile de lucru din afara birourilor. Aproximativ 1 din 5 lucrători la distanță sunt de părere că activitățile lor online nu privesc pe nimeni.*

Cisco a publicat astăzi rezultatele unui al doilea studiu internațional privind lucrătorii la distanță și comportamentul lor online, relevând o percepție deconcertantă a acestora asupra rolului managerilor IT, fapt care poate periclita securitatea companiilor și a persoanelor. Frecvent, rolul managerilor IT este considerat ca fiind unul reactiv și, în unele cazuri, mai lipsit de autoritate decât acela al managerilor non-IT.

Acest nou studiu include răspunsuri oferite de peste 1.000 de lucrători la distanță și 1.000 de decidenți în domeniul IT din 10 țări: Statele Unite, Marea Britanie, Franța, Germania, Italia, Japonia, China, India, Australia și Brazilia. Realizat în vara acestuia an de către o firmă independentă de cercetare a pieței, studiul se bazează pe rezultatele unui studiu anterior privind contradicțiile comportamentale ale lucrătorilor la distanță vizavi de securitate. Având drept „fundal” comportamentul riscant al lucrătorilor la distanță noul studiu a avut în vedere aceleași persoane, urmărind însă percepția acestora asupra rolului personalului IT în protejarea activităților lor. La rândul lor, profesioniștii IT și-au exprimat opiniile privind percepția utilizatorilor asupra rolului lor.

Răspunsurile oferite de cele două categorii de persoane interviewate constituie un semnal de alarmă pentru comunitatea IT globală. În 6 dintre cele 10 țări (inclusiv în Statele Unite), un număr sporit de lucrători la distanță consideră că managerii au mai multă autoritate de a controla comportamentul lor decât organizațiile IT. În cazul Franței, 38% dintre teleoperatori au declarat că acest comportament nu privește pe nimeni, iar 33% – că organizațiile IT au dreptul de a controla comportamentul online.

De asemenea, un număr sporit de lucrători la distanță din Australia, Brazilia, China și Marea Britanie consideră că managerii au mai multă autoritate decât organizațiile IT. India, Italia și Germania constituie o excepție; cu toate acestea, o treime dintre lucrătorii la distanță din Japonia și din Germania consideră, indiferent de poziția lor față de personalul IT, că responsabilitatea controlării comportamentului online revine managerilor. Toți cei interviewați nu sunt profesioniști în domeniul IT, acest lucru însemnând că managerii departamentelor de vânzări, de marketing, de contabilitate, de resurse umane, de servicii pentru clienți, de operații etc. sunt percepuți ca rivalizând sau eclipsând autoritatea managerilor IT în ceea ce privește administrarea comportamentului online al utilizatorilor.

13% dintre lucrători la distanță consideră că, în afară de manageri și de personalul IT, nimeni nu ar trebui să controleze modul de utilizare a echipamentelor IT ale companiilor. Această opinie a fost împărtășită de peste o treime dintre lucrătorii la distanță interviewați din Franța (38%) și din Italia (35%). În același timp, media globală a fost depășită și de Japonia (22%), de Statele Unite (14%) și de Australia (14%).

„Aceste rezultate evidențiază influența pe care o exercită diversele culturi sociale și comerciale asupra percepției și a comportamentului. De exemplu, în Germania, 71% dintre lucrătorii la distanță au fost de acord că personalul IT ar trebui să le monitorizeze comportamentul online, în timp ce o treime a considerat că această responsabilitate ar trebui să revină și managerilor. Pe de altă parte, 1 din 4 lucrători la distanță consideră că și colegii de muncă ar trebui să joace un anumit rol în această monitorizare. Numeroși respondenți germani consideră că întreg personalul companiilor este răspunzător de securitatea informațiilor.” (Jeff Platon, Vice President, Security Solutions Marketing, Cisco Systems)

De asemenea, Jeff Platon consideră că, în celelalte țări, responsabilii cu securitatea informațiilor se confruntă cu o altă problemă – restabilirea rolului personalului IT vizavi de utilizatorii finali. Pentru majoritatea profesioniștilor IT interviewați, percepția lucrătorii la distanță asupra rolului pe care ar trebui să-l

joace nu a constituit o surpriză. 53% dintre acești profesioniști IT cred că utilizatorii nu consideră că personalul IT are dreptul să cunoască modul în care sunt utilizate echipamentele companiilor. Rezultatele studiului arată că această situație este diferită numai în India și în Brazilia.

În opinia lui John Stewart (Chief Security Officer, Cisco Systems), această percepție nu constituie o problemă, ci, mai degrabă, o oportunitate pentru profesioniștii IT de a-și asuma rolul de consilieri de încredere în ceea ce privește securitatea informațiilor.

„Personalul IT înțelege că angajații cunosc existența problemelor legate de securitate, însă, frecvent, nu conștientizează riscurile generate de comportamentul lor online. Cheia soluționării acestei probleme o constituie educația și conștientizarea riscurilor. Personalul IT și responsabilii cu securitatea informațiilor companiei trebuie să colaboreze cu membrii conducerii în vederea educării angajaților în ceea ce privește riscurile potențiale și responsabilitățile care trebuie asumate. Deși este imperativ ca managerii IT să identifice tehnologiile proactive necesare protejării organizațiilor împotriva riscurilor de securitate – riscuri care apar întotdeauna acolo unde numeroase persoane cu diverse niveluri de pregătire profesională se conectează la rețea –, dezvoltarea unei culturi bazate pe cunoașterea problemelor de securitate nu se poate realiza decât în condițiile combinării produselor de comunicare proactive cu educația.

Conform opiniei lui Jeff Platon, rezultatele primului studiu publicat la începutul acestei luni (*Actions Speak Louder Than Words: Despite Claiming Security Awareness, Many Remote Workers Engage in Risky Online Behavior – Faptele sunt mai grăitoare decât vorbe: în pofida comportamentului online riscant, numeroși teleoperatori se angajează în activități online riscante* – [http://newsroom.cisco.com/dlls/2006/prod\\_100906.html](http://newsroom.cisco.com/dlls/2006/prod_100906.html)) confirmă opinia anterioară a lui John Stewart.

„Conform primului studiu, două treimi dintre lucrătorii la distanță intervievați au susținut că sunt conștienți de existența problemelor legate de securitatea informațiilor. Cu toate acestea, numeroși dintre aceștia au recunoscut că au un comportament riscant atunci când utilizează echipamentele companiei. Prin urmare, se poate observa existența unei contradicții între conștientizarea riscurilor de securitate și comportamentul online.”

Comportamentul online riscant include piratarea rețelelor wireless ale vecinilor, deschiderea mesajelor de e-mail suspecte, accesarea fișierelor companiilor prin intermediul unor echipamente personale și partajarea calculatoarelor de la locul de muncă cu persoane din afara companiilor. Atunci când au fost întrebați de ce au un astfel de comportament online riscant, lucrătorii la distanță au oferit o gamă largă de explicații, dintre care enumerăm: „Nu cred că acest comportament generează riscuri de securitate.”; „Responsabilii companiei la care sunt angajat nu cunosc sau nu acordă o prea mare importanță comportamentului meu online.”; „Și colegii mei de muncă procedează la fel.”

„Contradicția dintre conștientizarea riscurilor de securitate și comportamentul online al lucrătorilor la distanță, rațiunile pe care se bazează acțiunilor lor și percepția asupra rolului personalului IT constituie motive suficiente ca managerii diverselor departamente să-și reevalueze rolul de consilieri în domeniul securității informațiilor la nivelul organizațiilor din care fac parte. Acest studiu demonstrează cu claritate că securitatea este o responsabilitate a tuturor. Personalul IT are oportunitatea – și, în același timp, obligația – să schimbe percepția utilizatorilor asupra rolului lor în asigurarea securității informațiilor și să promoveze corelarea problemelor generate de riscurile de securitate cu acțiunile teleoperatorilor.

Impulsionarea acestei schimbări necesită acțiuni diverse.” (John Stewart) Printre acestea se numără formarea unui front comun la nivelul conducerilor companiilor, numirea unor așa-numiți „ambasadori ai securității”, derularea de programe de instruire, realizarea de comunicații interne integrate, comunicarea la nivel global cu asigurarea relevanței regionale și oferirea de recompense evidente teleoperatorilor cu un comportament online adecvat.

„Trebuie spuse câteva lucruri despre evoluția de la „acțiunile din spatele biroului” și comunicarea reală cu oamenii. Majoritatea echipelor responsabile cu securitatea IT au avut, până acum, un rol „reactiv” și „discret”, fapt care le-a împiedicat să demonstreze conducerilor companiilor că sunt capabile să prevină deficiențele de productivitate și pierderile de date. Oferind consultanță și educând utilizatorii finali, personalul IT poate transforma această imagine, devenind o sursă de încredere pentru instruirea în domeniul securității – adică exact ceea ce doresc managerii și necesită companiile.” (John Stewart)

Pentru informații suplimentare despre rezultatele globale și cele specifice pentru toate cele 10 țări, accesați pagina Web conținând ambele studii de la adresa:

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking\\_solutions\\_white\\_paper0900aecd8054581d.shtml](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd8054581d.shtml)

### **Despre Cisco**

Cisco Systems (NASDAQ: CSCO) este liderul mondial în comunicațiile Internet. Știrile și informațiile Cisco sunt disponibile la adresa Web <http://www.cisco.com>. Pentru știri de ultimă oră, accesați pagina Web de la adresa <http://newsroom.cisco.com>. Echipamentele Cisco pentru zona europeană sunt furnizate de Cisco Systems International BV, o filială în proprietate exclusivă a Cisco Systems, Inc.

###

Cisco, Cisco Systems și sigla Cisco Systems sunt mărci înregistrate ale Cisco Systems, Inc. și/sau ale societăților afiliate din SUA și din alte câteva țări. Toate celelalte mărci menționate în acest document sunt proprietatea firmelor respective. Utilizarea termenului de partener nu implică o relație de parteneriat între Cisco și oricare altă companie. Acest document face parte din Informațiile Publice Cisco.