October 21, 2013

Fortinet Global Survey Shows Generation Y's Hardening Stance Against Corporate BYOD/Bring-Your-Own-Cloud Policies as Emerging Technologies Enter the Workplace

Up to 51% of 21-32 Year Old Employees Would Contravene Company Policies Restricting Use of Own Devices, Cloud Storage and Wearable Technologies for Work

SUNNYVALE, CA -- (Marketwired) -- 10/21/13 -- Fortinet® (NASDAQ: FTNT) -- a global leader in high-performance network security -- has published global research revealing the growing appetite of Generation Y employees to contravene corporate policies governing use of own devices, personal cloud storage accounts and new technologies such as smart watches, Google Glass and connected cars. Based on findings from an independent 20-country survey of 3,200 employees aged 21-32 conducted during October 2013, the research showed a 42% increase in the willingness to break usage rules compared to a similar Fortinet survey conducted last year[1]. The new research also describes the extent to which Generation Y have been victims of cybercrime on their own devices, their 'threat literacy' and their widespread practice for storing corporate assets on personal cloud accounts.

Strong Trend of Contravention
Despite respondents' positivity about their employers' provisions for BYOD policy, with 45% agreeing this 'empowers' them, in total, 51% stated they would contravene any policy in place banning the use of personal devices at work or for work purposes. This alarming propensity to ignore measures designed to protect employer and employee alike carries through into other areas of personal IT usage. 36% of respondents using their own personal cloud storage (e.g. DropBox) accounts for work purposes said they would break any rules brought in to stop them. On the subject of emerging technologies such as Google Glass and smart watches almost half (48%) would contravene any policy brought in to curb use of these at work.

Wearable Technology Set to Enter the Workplace
When asked how long it would take for wearable technologies such as smart watches and Google Glass to become widespread at work or for work purposes, 16% said 'immediately' and a further 33% when costs come down. Only 8% of the entire sample disagreed that the technologies would become widespread.

Widespread Use of Personal Cloud Accounts for Sensitive Corporate Data
89% of the sample has a personal account for at least one cloud storage service with DropBox accounting for 38% of the total sample. 70% of personal account holders have used their accounts for work purposes. 12% of this group admits to storing work passwords using these accounts, 16% financial information, 22% critical private documents like contracts/business plans, while a third (33%) store customer data.

Almost one third (32%) of the cloud storage users sampled stated they fully trust the cloud for storing their personal data, with only 6% citing aversion through lack of trust.

Threat Literacy Required as Survey Reveals Attacks Really do Happen
When asked about devices ever being compromised and the resulting impact, over 55% of responses indicated an attack on personally owned PCs or laptops, with around half of these impacting on productivity and/or loss of personal and/or corporate data. Attacks were far less frequent on smartphones (19%), with a slightly higher proportion resulting in loss of data and/or loss of work productivity than on PCs/laptops, despite the sample reporting a higher level of ownership of smartphones than for laptops and PCs. The same percentage was observed for tablets (19%), but with greater consequences, since 61% of those attacks resulted in significant impact.

Among one of the worrying findings of the research, 14% of respondents said they would not tell an employer if a personal device they used for work purposes became compromised.

The research exercise examined 'literacy levels' for different types of security threat, with the results revealing two opposing extremes of ignorance and enlightenment, separated by an average of 27% with minimal awareness. Questioned on threats like APTs, DDoS, Botnets and Pharming, up to 52% appear completely uneducated on these types of threats. This represents an opportunity for IT departments to provide further education around the threat landscape and its impact.

The survey also hinted at a direct correlation between BYOD usage and threat literacy, i.e. the more frequent the BYOD habit, the better a respondent's understanding of threats. This represents a positive finding for organizations when considering if/when to bring policies in alongside training on the risks.

"This year's research reveals the issues faced by organizations when attempting to enforce policies around BYOD, cloud application usage and soon the adoption of new connected technologies," said John Maddison, vice president of marketing for Fortinet. "The study highlights the greater challenge IT managers face when it comes to knowing where corporate data resides and how it is being accessed. There is now more than ever a requirement for security intelligence to be implemented at the network level in order to enable control of user activity based on devices, applications being used and locations."

"It's worrying to see policy contravention so high and so sharply on the rise, as well as the high instances of Generation Y users being victims of cybercrime," continued John Maddison. "On the positive side, however, 88% of the respondents accept that they have an obligation to understand the security risks posed by using their own devices. Educating employees on the threat landscape and its possible impact is another key aspect for ensuring an organization's IT security."

Note for Editors
The Fortinet Internet Security Census 2013 was a research exercise undertaken between October 7-13, 2013 on behalf of Fortinet by independent market research company Vision Critical. The survey involved 3,200 university graduate level individuals aged 21 to 32 and in full time employment, who own their own smartphone, tablet or laptop.

*20 territories participated in the survey: Brazil, Canada, Chile, China, Colombia, France, Germany, Hong Kong, India, Italy, Japan, Korea, Mexico, Netherlands, Poland, Russia, Spain, Taiwan, UK and USA.

Follow Fortinet Online:
Twitter at: www.twitter.com/fortinet
Facebook at: www.facebook.com/fortinet
YouTube at: http://www.youtube.com/user/SecureNetworks
LinkedIn at: http://www.linkedin.com/company/fortinet
G+ at: https://plus.google.com/+fortinet

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FTNT-O

[1] Fortinet Internet Security Census 2012 polled 3,872 20-29 year old employees in 15 countries and asked the exact same question.

Media Contact:
Rick Popko
Fortinet, Inc.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet