Intelligent ID – *User Activity Monitoring*

Massachusetts' UMass Memorial Medical Group *recently acknowledged that a former employee may have inappropriately accessed patient information.*

Helen Wong, a former VIP host at ***Maryland Live Casino*** *is suspected of copying a list of its 1,000 best customers before taking at job a dozen miles away at Horseshoe Casino*

Anthem*, the insurer giant, had their database was compromised that contained up to 80 million customer records that included names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data.*

Sony *believed early on someone on the inside had to help find the information released in the Sony leak*

CONVERGENCE

Intelligent ID – User Activity Monitoring
Insider Threat – #1 Security Risk

WHAT STUDIES ARE SAYING...

- "A study by SolarWinds and Market Connections showed that almost two thirds, 64 percent, of the federal IT professionals polled said intentional malicious insider attacks were as damaging or more damaging than malicious external threats, such as terrorist attacks or hacks by foreign governments. Almost 60 percent, however, said breaches caused by accidental or careless insiders could be as damaging as or more damaging than those caused by malicious insiders."

- "Health Data Management reported that the most important technical safeguards for PHI on mobile devices are encryption and endpoint security software…"

- "According to enterprise data security provider Vormetric, 93 percent of US corporations are vulnerable to threats -- from the inside. The security landscape has changed rapidly in the last few years, with high-profile data breaches attacking companies indiscriminately."

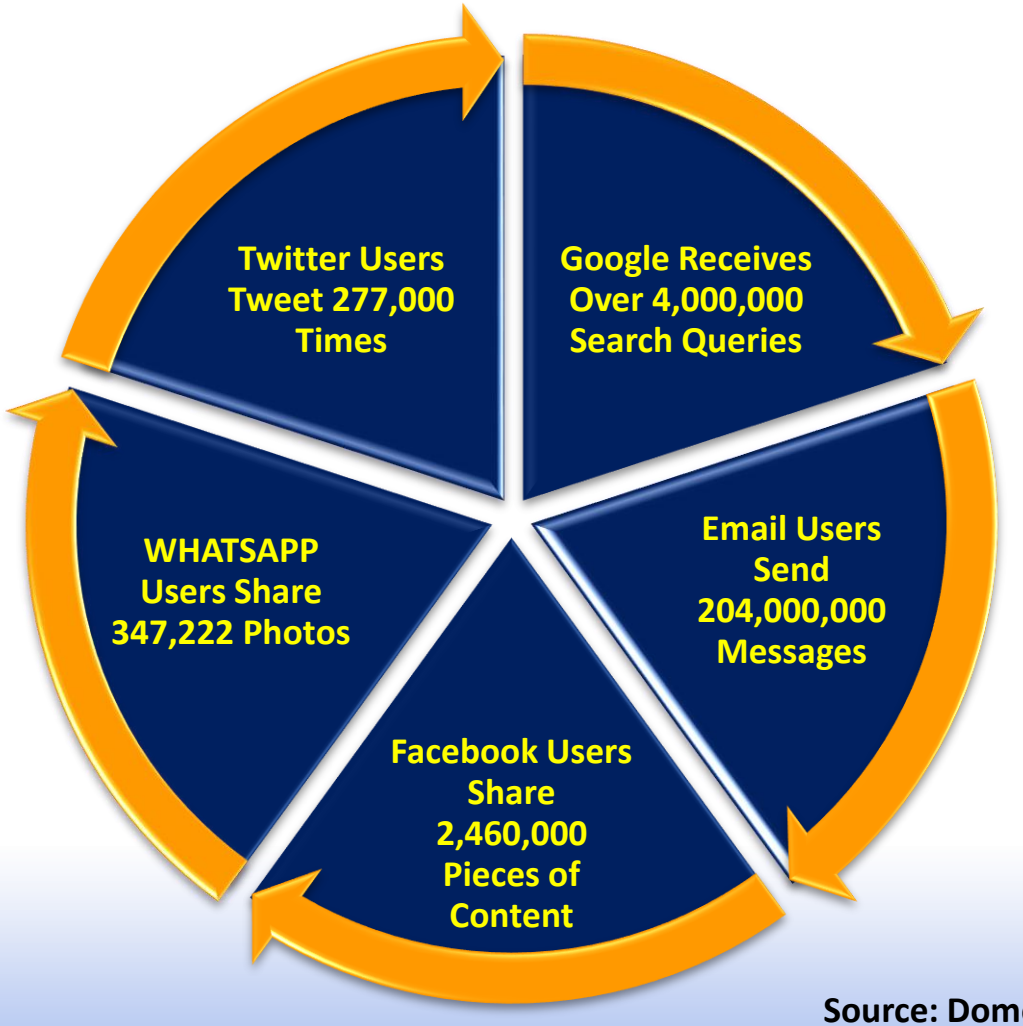
- "Insider threat is traditionally thought to be malicious employees with access to critical data and systems as part of their work, but a major shift is occurring as a result of huge data breaches like the one Target suffered, where compromised credentials of a supplier were used as the attack vector…" according to a leading CEO.

CONVERGENCE

Intelligent ID protects your employee's data habits from hurting the company

Every Minute of Every Day

"Privileged users or employees who have high-level access to very sensitive data, who are considered to be the company's greatest threat"



"93 percent of IT personnel think their company is at risk from an insider threat"

"Enterprises are looking for an integrated suite… this may include other related functions, such as endpoint encryption, browser security, and endpoint Data Loss Prevention (DLP) for simplified management and integrated visibility"

"There is a need to implement stringent control on all these devices to keep sensitive company information secure"

CONVERGENCE

Source: Domo, Inc., April 2014

Convergence Technology Consulting
360o protection

- ***Protect Company Intellectual Property (IP)***
  - Source code, manufacturing designs, customer contact lists
  - Patented techniques, confidential documents
- ***Protect Customer Sensitive Information***
  - Personal identifiable or health information (PII / PHI)
  - Payment information such as credit cards, bank accounts, etc.
- ***Protect Employee Welfare***
  - Identify and prevent violent actions
  - Identify and address potential harassment concerns
- ***Ensuring Corporate Compliance***
  - HIPAA / SOX federal compliance initiatives
  - Internal corporate compliance policies