Emerging Trends

Bill Claycomb
Lead Research Scientist - CERT Enterprise Threat and Vulnerability Management Program

Bill Claycomb is the Lead Research Scientist for the CERT Enterprise Threat and Vulnerability Management program at Carnegie Mellon University's Software Engineering Institute. His primary research topic is the insider threat; current work includes discovery of insider threat behavioral patterns and corresponding sociotechnical countermeasures

Andy Moore
Lead Researcher - CERT Insider Threat Center, Senior Member of the Technical Staff

Andy Moore is a lead researcher in the CERT Insider Threat Center and Senior Member of the Technical Staff at Carnegie Mellon University's Software Engineering Institute. He explores ways to improve the security, survivability, and resiliency of enterprise systems through insider threat and defense modeling, incident management, and architecture engineering and analysis.

Topics

- The Expanding Complexity of Insiders
- Cloud Computing
- Mobile Devices
- Social Networking and Social Engineering
- Future Threats

The Expanding Complexity of "Insiders"

The Expanding Complexity of "Insiders"

Area	Description
Collusion with outsiders	Insiders recruited by or working for outsiders, including organized crime and foreign organizations or governments
Business partners	Difficulty in controlling/monitoring access to your information and systems by "trusted" business partners
Mergers & acquisitions	Heightened risk of insider threat in organizations being merged into acquiring organization
Cultural differences	Difficulty in recognizing behavioral indicators exhibited by insiders working for US organizations who are not US citizens
Foreign allegiances	US organizations operating branches outside the US with the majority of employees who are not US citizens
Technology Advances	New and emerging technology often provides additional attack paths for insider threats that are difficult to detect

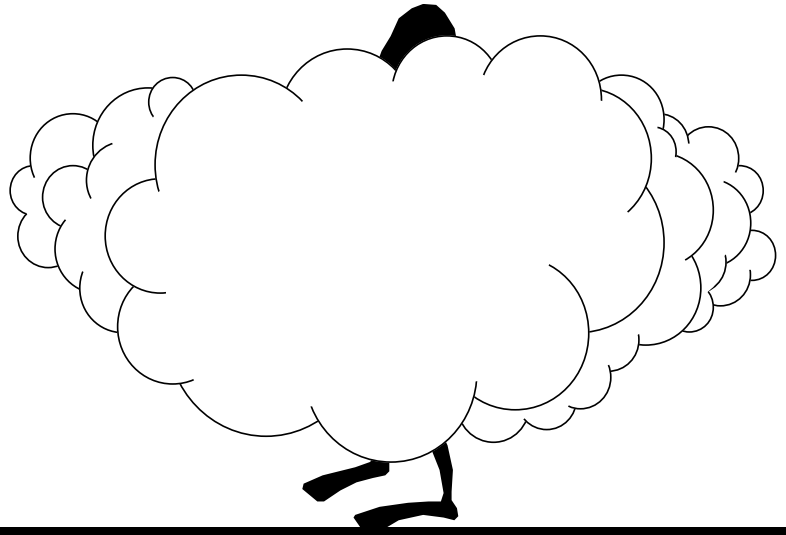
Cloud Computing and Insider Threats

Insider Threats in the Cloud

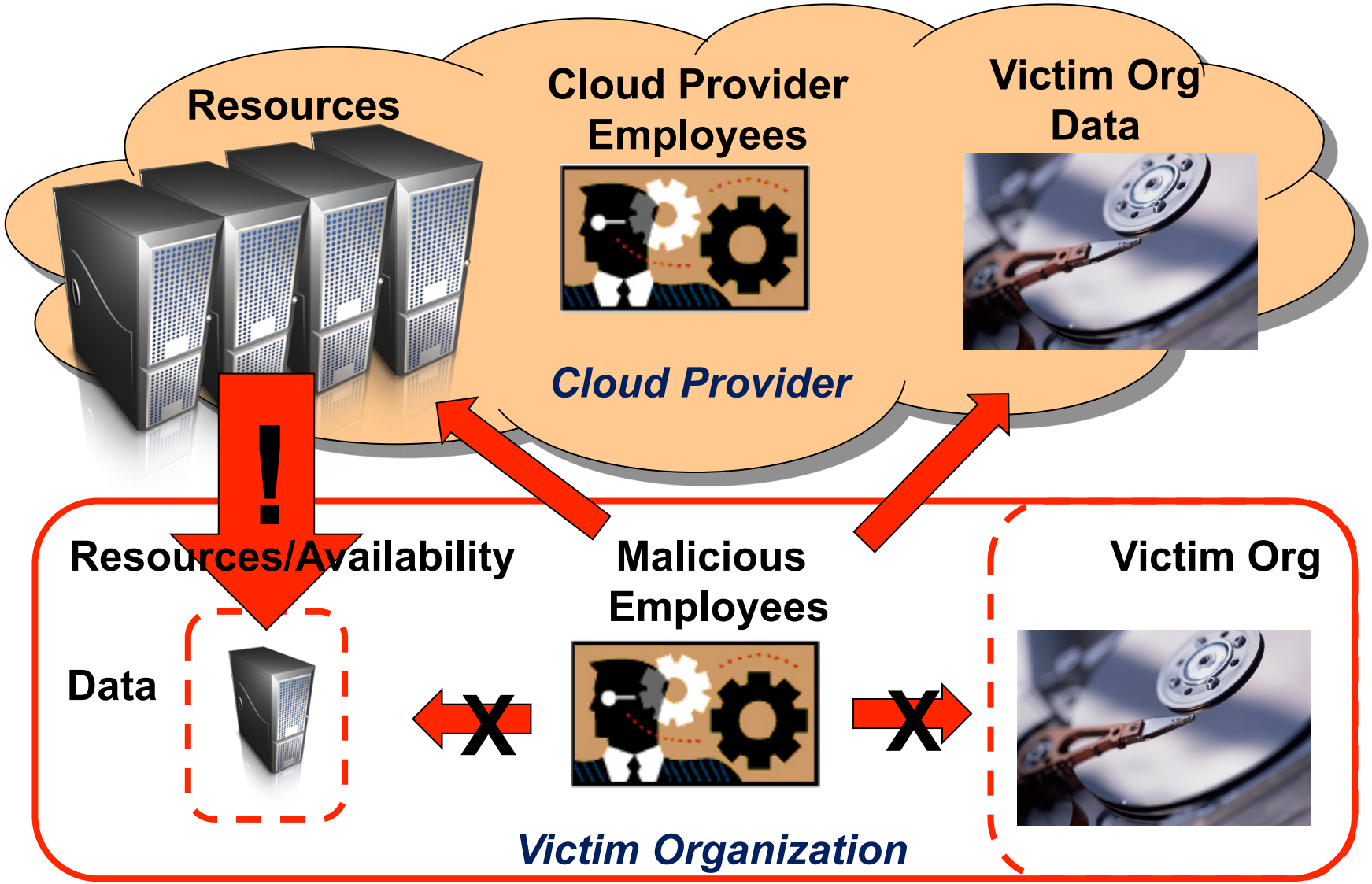
Identified by Cloud Security Alliance (CSA) “Top Threats to Cloud Computing, v1.0”

- Malicious insider working for cloud provider

But there are other insider threats related to cloud computing…



Provider / Organization Relationship



Cloud-Related Malicious Insider Threats

Malicious Cloud Provider Employee

- *Rogue Administrator*
  - We've seen cases of insider threats from trusted business partners
  - True examples of cloud service providers are rare, but do exist
  - Important to weigh the risks carefully; the provider has much to lose as well

Cloud-Related Malicious Insider Threats

Malicious Local Employee

- Attacking the organization's data in the cloud
  - Example weakness: the organization may not have immediate control of data/services in the cloud
    - Effecting change quickly may be difficult
      - Example case: Email provider
  - Access control models may be different
- Using the cloud to attack the organization
  - Example weakness: the cloud is a very powerful tool; and a very powerful weapon, what if it is turned back on the org itself?

Protecting Against Malicious Insiders

- Those that exploit weaknesses in the Cloud
  - Diligence in planning during implementation, transition, migration, and maintenance of cloud services
  - Clear plans for handling incidents
    - Including authentication and authorization between org and host provider
- Those that use the Cloud against you
  - Host-based and network-based monitoring
  - Limit access to potential exfiltration resources
  - Create separate environments for external communication

Mobile Devices

Mobile Devices

- Organizations moving to a more mobile workforce
  - Remote access via smartphones and tablet computers
  - Can enhance productivity
- Features of mobile devices
  - Cameras, microphones, other apps
  - Mass storage
  - Remote access
  - Wireless capabilities (Wi-Fi, Bluetooth, cellular, …)
- May be owned by employee or by employer
- Employees want to choose the device they use for work[1]

[1] Hamblen, Matt. *Workers Want to Choose Their Mobile Devices, Survey Finds.* (2011). https://www.computerworld.com/s/article/9218693/Workers_want_to_choose_their_movile_devices_survey_finds

Risks of Mobile Devices

- Emerging attack platform for malicious insiders
- Employee-owned
  - Limited monitoring capabilities by the employer
  - Many different paths for data exfiltration
    - Camera and microphone
    - Remote access and other applications
    - Wireless capabilities (including those outside the ability of the organization to monitor, such as MMS)
    - Mass storage capabilities
  - May allow access to both corporate and personal email accounts
    - Unintentional data leakage via personal accounts may occur

Risks of Mobile Devices

- Employer-owned
    - Still has the capability to exfiltrate sensitive information
    - May be easier to monitor for unauthorized use
- Compromised mobile devices may allow an external attacker access to internal corporate resources
    - Possibly remote access to the user desktop
- Devices may sync data to locations with inadequate security
    - Cloud storage
    - Social media services
    - Personal computers

What You Should Do

- Organizations should strongly consider limiting remote access by mobile devices
    - At the very least, limit mobile device access/use in sensitive areas.
- If possible, allow remote access from corporate-owned devices only
- Monitor all remote access transactions as closely as possible
- Disable remote access and collect company devices immediately upon insider termination

Social Networking & Social Engineering

Social Networking

"A social network is a social structure made up of a set of social actors (such as individuals or organizations) and a set of the dyadic[1] ties between these actors." - Wikipedia

Possible areas of concern related to insider threats:

- Online Social Networking
- Non-technical Social Networking
  - Family or culture

[1] In sociology, a dyad (from Greek dýo, "two") is a group of two people, the smallest possible social group. - Wikipedia

Risks of Online Social Networking

- Personal information can be used to identify likely targets of attack within a company (i.e. for spear-phishing, etc.)
- May also help identify likely candidates for collusion
  - Disgruntled employees
- Data loss may occur intentionally or accidentally
- Employees may not realize the potential for data loss or harm to the organization
  - Social networking profiles may enable attackers to hijack user accounts
  - False information is hard to dispel[1]
- Data loss may be difficult to detect

[1] Stephanie Chen, CNN. "Workplace rants on social media are headache for companies." http://www.cnn.com/2010/LIVING/05/12/social.media.work.rants/index.html. May 12, 2010.

What Should You Do

All organizations should consider

- Establishing social media policy that defines acceptable use
- Including social media awareness training in training program
- Encouraging users to report suspicious contacts to information security team

Large organizations should consider

- Monitoring use of social media across organization, as approved by legal counsel

Use Caution in Control and Monitoring

- Organizations must ensure legality of social media policies
  - From a 2012 National Labor Relation Board report[1]
    - Avoid policy language that prohibits posts discussing non-public information or negative comments about employer
- Monitoring social media use should be done with caution
  - Avoid penalizing or firing employees for discussing work conditions, such as pay, online
  - Social media may inform an organization about an employee's protected status, opening the door to discrimination lawsuits
  - Some states have enacted legislation restricting employers' monitoring of employee use of social media
    - Some employers were asking for employees/candidates social networking site passwords

Other Types of Social Networking

- Organizations operating branches outside their own country must consider the insider threats posed by employees with allegiance to another country.
- Competing loyalties, coupled with the recruitment of employees in U.S. businesses by foreign nations or organizations, make the theft of intellectual property (IP) a potent threat for organizations that rely on IP for a competitive advantage
    - Many cases of IP theft in the CERT Insider Threat Database were associated with foreign social network connections.

[1] Verizon. "The 2013 Data Breach Investigations Report."
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Social Networking Wrap-Up

- See CERT's Common Sense Guide to Mitigating Insider Threats, 4th Edition, practice 18 for more info:
  - http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

Social Engineering

- Seen in many of the cases in CERT's database
  - Fraud
  - Organized Crime
  - Sabotage
- Tactics often used[1]
  - Phishing, doxing (document tracing), and watering hole attacks
- Features prominently in several recent high-profile attacks
  - Employees tricked into unlocking accounts, revealing passwords, opening infected attachments or web sites, etc.

[1] Verizon. "The 2013 Data Breach Investigations Report."
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Social Engineering

- A 2012 Ponemon study shows “Phishing & social engineering” attacks were experienced by 38% of respondents[1]
- The 2013 Verizon Data Breach Report[2] reveals
  - 29% of breaches studied leveraged social tactics
    - A fourfold increase from 2012
  - Email (79%) and in-person (13%) were the most common vectors of social engineering attacks
  - Executives and managers were the most likely targets identified (27% total), followed by former employees (10%)

[1] Ponemon Institute. “2012 Cost of Cyber Crime Study: United States.”
http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf
[2] Verizon. “The 2013 Data Breach Investigations Report.”
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Future Threats

Future Threats

- New technologies that enable insider attacks
  - USB device emulators[1]
- New vulnerabilities to existing (and embedded) technology
  - Eavesdropping on cell phone signal boosting devices[2]

[1] "Hacking with Keyboard Emulators"
http://www.h-online.com/security/news/item/Hacking-with-USB-keyboard-emulators-1172612.html
[2] Jim Finkle, Reuters. "Researchers hack Verizon device, turn it into mobile spy station"
http://www.h-online.com/security/news/item/Hacking-with-USB-keyboard-emulators-1172612.html

Contacts

William R. Claycomb
Lead Research Scientist
- Enterprise Threat and Vulnerability Management
Office: 412.268.8931
Email: claycomb@cert.org

Andrew P. Moore
Lead Researcher
- Insider Threat Research
Office: 412.268.5465
Email: apm@cert.org

CERT, Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0000553