This is the published version of a paper published in.

Citation for the original published paper (version of record):

Magnusson, L. (2013)
HR Access: a key to better InfoSecurity

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-77422
COMPLIANT CLOUD SERVICES: RAISING THE BAR

Cloud providers may claim to be secure, but are they truly compliant?
Compliant Cloud Services: Raising the Bar
Cloud providers may claim to be secure, but are they compliant?
BY CRYSTAL BEDELL

Securing Today’s Social Graces
Social media is the must-have technology to stay competitive. Managing and securing it is the more difficult must.
BY PETER FRETTE

Practice What You Preach
Leading by example can make a difference in how well employees adhere to security policies and procedures.
BY COLLEEN FRYE

Cyber Criminals and Clouds: Get Certified
Executive Letter
From the desk of (ISC)²’s Director of Global Development.

The True Value of Face Time
Moderator’s Corner
Highlights from (ISC)²’s event moderator, Brandon Dunlap.

FYI
Member News
Find out the latest news and announcements about (ISC)² and its members.

(ISC)² Security Congress 2013 At A Glance
Sessions and Tracks for the 3rd annual (ISC)² Security Congress in Chicago, Ill., U.S.A. September 24-27.

Seal of Approval
Q&A
George Japak, managing director, ICSA Labs, discusses testing, certification and security challenges.

Raising Cyber Security Awareness for Students
Chapter Passport
The (ISC)² Manitoba/Saskatchewan Chapter launches the Canadian Cyber Defence challenge.

HR Access: Key to Better InfoSecurity
Global Insight
IT budgets are best spent on core operations rather than audits. BY LARS MAGNUSSON, CISSP
HR Access: Key to Better InfoSecurity?

HAVING WORKED as an information security officer for more than a decade, I’ve seen my share of audits and tried to rectify the deficiencies that were found. This has made me think about how to improve processes, focusing less on corrective actions and more on getting it right from the start.

More recently, I’ve realized that the same six basic audit issues are cropping up:
1. Incorrect access rights (account)
2. No systematic responsibility for accesses (account)
3. Who did what, when (also known as segregation of duty)
4. Lacking corrective actions/follow-up (management)
5. Lacking documentation of decisions (management)
6. Faulty code, patching, or non-best practice (management)

The first two issues (incorrect access rights and no systematic responsibility for accesses) and partially the third issue (who did what, when) have a common denominator: individuals are accessing the IT systems. Such individuals comprise employees, consultants, external partners, and prospective customers.

Any organization, private enterprise or public management, should have some form of legal agreement or policy regulating such access. Such legal policies, whether in the form of employee information or temporary work contracts, are usually handled by human resource organizations.

HR manages our personnel resources, though often consultants and external personnel are not handled by HR. However, HR is capturing information on new employees, such as their titles, roles, job changes, prolonged absences, retirement, and permanent leave.

Our HR systems are written to handle this information, since they handle the legal implications of such changes. So, why not let HR (if it is not already) also take care of consultants and external users? This means all personnel information would be stored in one place, with valid dates of hires, reviews, and terminations.

You are probably thinking, what does this have to do with information security?

This data may be what is missing when it comes to access control processes: getting a heads up about completed or pending changes, triggering faltering access reviews that we pay for in audits.

I have yet to meet an information security professional who has not experienced the issue of access/authentication control. We make grand technological schemes to fix access control. However, the biggest issues are accounts that are not closed after an employees or contractors leave, change positions, or go on prolonged leave. My guess is that about half of all audit issues are due to incorrect access.

With a single financially and legally maintained source of data like HR, how much simpler would it be to make a trustworthy access control process? It would be efficient to have that nightly batch looking at advertised HR changes and flagging affected accesses to system owners/managers for review.

If we could curb incorrect accesses, we would likely decrease a large number of internal misuse. We would also see faster audits, resulting in fewer embarrassing errors.

Bottom line: Spend less money on audits and corrective actions; money is better spent on developing core operations. (§)

Lars Magnusson, CISSP, is a senior information security consultant and cloud enterprise architect, and previously an ISO within the Swedish automotive industry. He is based in Kalmar, Sweden, and can be reached at larsmn@hotmail.com.