medco®

Does Your House Have Lions?

Controlling for the risk from trusted insiders

Marcel-Franck Simon, CISSP

(with apologies to Rahsaan Roland Kirk)

The Trusted Insider Conundrum
You can’t live without them

Some people must have privileged access to systems

- System administrators , NOC staff, application-support staff…

You can’t really take away this privileged access

- Because then they can’t do their job
  - Or the job becomes significantly harder and more expensive
- Trying will just result in an impasse some day at 3AM
  - One with privilege is not available, one available lacks privilege…

Rogues among them can do damage *and* cover their tracks

- They know how the infrastructure is put together
- And they can subvert your controls

The Trusted Insider Conundrum
So how do you live with them?

Most of them are not rogues

- Treating them as such reduces their productivity
- And / Or annoys them so much that they quit
  - And you're stuck with staffing costs, loss of institutional memory…

But human nature says one *will* go rogue some day

- And you can't reliably predict who that one will be

How do you protect against rogues without crippling non-rogues' ability to do their job?

Defense in Depth or,
There is no silver bullet

Many controls are more secure than one

- Just as many thin clothes warm better than one thick one

Many controls cover infrastructure more completely

- Some overlap between controls is a Good Thing™!

Many controls are more effective overall

- Or, a given level of effectiveness costs less to achieve

Defense in Depth or,
There is no silver bullet

Multiple control *types,* multiple control *objectives*

Control types

- Policy
  - To set accountability, define the bounds of acceptable behavior
- Procedural
  - To guide and constrain day-by-day activities
- Technical
  - To support and implement the others

Control objectives

- Prevention
- Detection
- Investigation
- Recovery

What’s with this word ‘control’?

From The Institute of Internal Auditors (IIA, www.theiia.org)

- **Control:** A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

Process, not technology

- Because security is a ‘how’ not a ‘what’

Reasonable assurance, not ironclad guarantee

- Multiple controls, in layers, increase
  - *Reasonableness*, limiting effort required for operational compliance
  - *Assurance*, from greater overall coverage and effectiveness

Policy vs. Standard vs. Communication

Policy is “the law”

- General
- Changes rarely
  - Review annually, change only if necessary
- Requires interpretation
- Endorsed and reinforced by senior management

Resource: *SANS Policy Project http://www.sans.org/resources/policies/*

Policy vs. Standard vs. Communication

Standards are “regulations”

- Define acceptable “what” and “how”
  - Support more than one option if possible
  - But not more than necessary
- Technical and specific
  - Guidance to process or technology implementers and operators
  - Use ‘requirement-speak’ (distinguish *shall* from *should* from *may*)
- Evolve with business and technology
  - Review and update as needed
  - Needs update if requires constant explanation

Policy vs. Standard vs. Communication

Communications are “glossy booklet”

- Announcement messages
  - To foster awareness of a specific issue
- Aimed at end-users
  - Techno-speak is the enemy!
- Simplified, prescriptive information
  - “What you need to know”
  - “What you must do”
  - “What you must avoid”
- Validate effectiveness periodically
  - Recertification, polls, quizzes, …

Policy Controls - Recovery Objective

This clause belongs in every security policy

- *Failure to comply with this policy may result in disciplinary action up to and including termination of employment*
- Otherwise the policy cannot be enforced
- Any disciplinary action can be contested as arbitrary
  - Wrongful-termination lawsuits are no fun
  - Having to pay damages to someone even less so

If you really want to get aggressive

- Add *and referral to law enforcement agencies*
  - Human Resources will likely not agree to this
  - It’s not really necessary anyway

Policy Controls - Prevention Objective

Employee Screening

- Drug tests, background checks

Really necessary?

- Regulatory and contractual requirements
  - HIPAA – Health-care sector
  - GLBA – Financial-services sector
  - PCI DSS – Credit-card handling and transaction processing
- Audit requirements
  - If your customers must screen, their auditors will demand it of you

How effective is it?

- One-time snapshot
- Backward-looking
- Will identify ‘red-flag’ cases

Procedural Controls

Document, Document, and then Document some more

- Formal written Standard Operating Procedures (SOPs)
  - Under change control by department owning the procedure
  - Reviewed not less than annually, updated as necessary
  - Document anything that gets done more than once
- And a Checklist for *every* instance of executing an SOP
  - Records *who* did *what when* with what *result*, and any *exceptions*
  - Keep for however long company records retention policy dictates

Seriously, document *everything!*

- Collectively, your SOPs completely describe how you do business
  - Server configuration and hardening, system monitoring, backup, firewall change control, log configuration / storage / analysis, `root` password management, UID creation, …

Procedural Controls

"Do I really have to do all this?"

- Yes
  - SOX and friends say so
  - As does effective BCP
  - Auditors expect and demand it
- Has other benefits
  - Helps new staff ramp up quickly
  - Simplifies audit response

Significant security benefit

- Systematic evaluation of operational processes
  - Identify dodgy existing practices, bake security into new practices
- Codifies *normal*, thus enables detection of *abnormal*

Procedural Controls - Many Objectives

Prevention

- Disallow unsafe or inappropriate practices
- Channel trusted users into secure practices
  - Routine, i.e. more likely to be followed

Detection and Investigation

- Checklists form a process-level audit trail
- Checklists support both detection and investigation
  - Depending on the extent of monitoring controls

Recovery

- Simpler to rebuild what is well-documented

Procedural Controls
Prevention Objectives

The Organizing Principle: **Separation of duties**

- No one person can have the power to alter or destroy data, applications, or systems, without being detected
- Therefore, rogue activity requires collusion to be undetectable
  - Difficult since most people are not rogues most of the time
  - Effective SoD controls deliver reasonable assurance

Procedural Controls
Prevention Objectives

Separation of duties: different task types, different owners

- Administrators: system vs. network
- System Administrators: Unix vs. Windows
- Network Administrators: switches and routers vs. firewalls
- Windows Administrators: servers vs. desktop
- Access Control: DBA vs. user provisioning
  - Yet another person or team *authorizes* access
- Application: developer vs. production support
- Application: developer vs. release or content management
- Data: developer vs. DBA
- Data location: production vs. development or QA environment
- And so on

Procedural Controls
Prevention Objectives

“Wow, this is really hard to do!”

- Yes, but absolutely necessary
  - SoD analysis tells you who can do what to your systems or data
- Without it, you don’t know what you don’t know
  - In other words, you grant trusted insiders privilege over **you**
- At minimum, perform SoD analysis to characterize business risk
- Remediate problems over time if can’t do it at once
  - SOPs provide an excellent vector for approaching remediation
  - **Caution**: business is at risk during “over time,” so don’t dilly-dally

Procedural Controls
Prevention Objectives

But, how to go about it?

- Geographical separation
  - Staff at different sites, even if on same team
- Organizational separation
  - The higher up the management chain the better
  - Manager sign-off on tasks
- Requires constant reinforcement
  - **Never** cut SoD corners, and call out those who do
- Supplement with job rotations…
  - The one rotating *in* inherits responsibility for violations
  - Creates incentive to ferret out problems
- … or mandatory time off
  - Compare audit trails closely during time off vs. normal, for unexpected differences

Procedural Controls
Prevention Objectives

The best possible preventive control: no access at all

- Even privileged users can’t copy or damage what’s not there

So unless you absolutely must, **don’t**

- Store it
- Process it
- Transfer it

Especially for regulated information such as

- Social security or credit-card numbers
- Other personal identification information
- Financial or health history

Procedural Controls
Detection and Investigation Objectives

Goal: record *all* security-significant activity

- In enough detail to answer:
  - *Who* did *what when* from *where* with what *result*, and was that result *allowed or disallowed*
  - OK to aggregate data from multiple systems, so long as answer is unambiguous

- Stored somewhere not accessible by the trusted insiders
  - Could be a system managed by *different* trusted insiders
  - Obvious attack vector, so perform careful SoD analysis

- Keep for however long company records retention policy dictates

Procedural Controls
Detection and Prevention Objectives

This means logs and more logs

- Collect and correlate records from multiple different sources
  - Servers, desktops, databases, applications, firewalls, routers/ switches, domain, email, building access, remote access…
- Configure so that turning off recording creates a record

Quick-scan logs regularly

- Minimum due-diligence detection of egregious rogue activity

Activity Monitoring
Not as simple as it sounds

On the one hand

- Why wait for the rogue to do damage?
- Management, customers, and auditors will all expect it

On the other hand

- Harder to do well than vendors claim or management believes
- Expensive in both dollars and time
  - Process multi-GB/day of logs in real time
  - Who does the monitoring, 24x7?
  - False positives, false negatives
- Quis custodiet ipsos custodes – who watches the watchers?
  - Now highly trusted insiders

Conclusion: define monitoring controls carefully

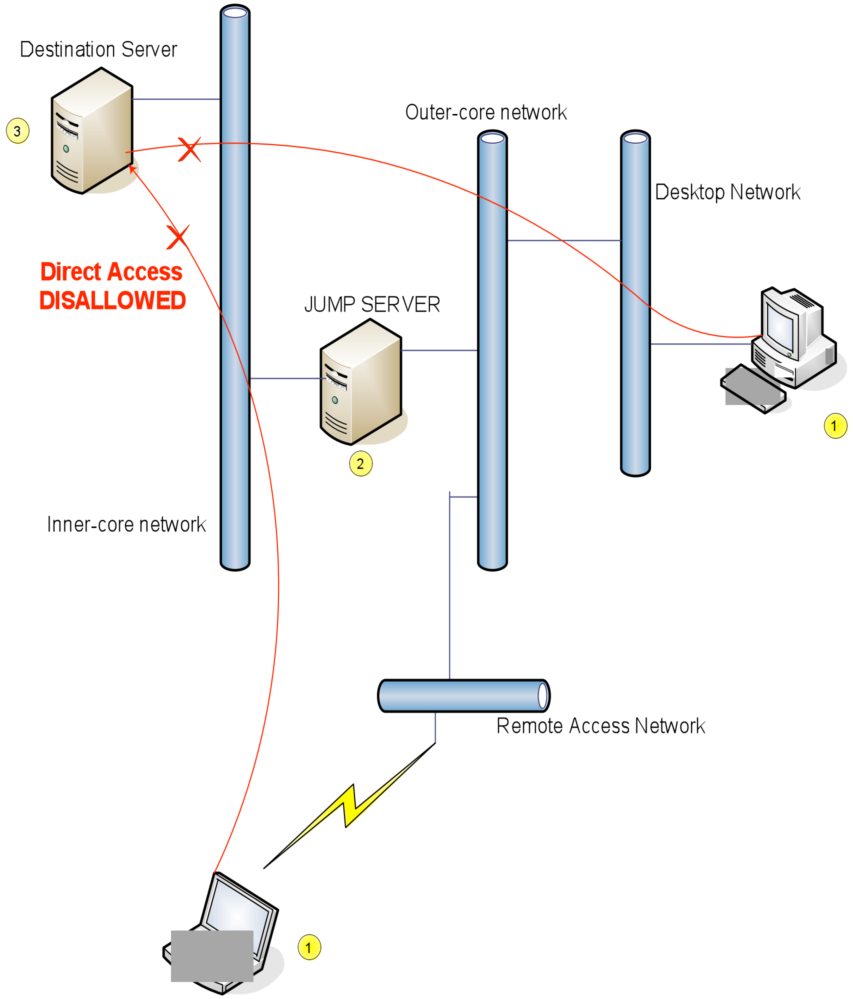
- Cost of implementing vs. cost of over-committing

Technical Control
Who logged into `root`?

Determining the *who* in “who did what…”

- Target activity likely performed by shared privileged ID
  - Such as `root` or `oracle` or similar
- Multiple privileged users have the capability
  - May even be logged in simultaneously
- Must track a privileged-ID session back to the initiating individual

Technical Control
Who logged into `root`? – The Jump Server



1) Login to desktop or remotely
   - Recorded by the domain

2a) SSH into Jump Server
   - Logged by `sshd` syslog
   - Including incoming PTY

2b) Obtain privilege using `sudo`
   - Logged by `sudo`

3) SSH to Destination Server
   - No password, `ssh` trusts
   - Logged by *from* `ssh` and *to* `sshd`

On Windows, VNC/SSH or RDP/SSL
   - 2 IDs: one normal, one privileged
   - Login to Jump Server with Priv-ID
   - VNC or RDP record to event log

Technical Control
Who logged into `root`? – The Jump Server

Jump Servers are very lightweight

- Proxy access to production
- Copy screen and keyboard bytes back and forth
- And log, of course

Different Jump Servers for different recording needs

- System administrator access to servers
- Network administrator access to networking devices
- Application production support access
- Vendor maintenance access
  - Control when vendor *can* access and when vendor *does* access
- Balance multiple servers vs. who manages them all
  - Separation of duties analysis, operational cost of managing

Procedural Controls
Investigation Objectives

What you really do with all these logs

- Answer "who did what when …" when something happens
  - Most recent logs are online, others recallable from backups

Prepare for investigations

- Correlate logs, regularly, to isolate certain types of activity
  - Same activity across different systems
  - Unexpected activity in one system
- Review these reports before diving into multi-GB raw logs
  - Correlate to scheduled change-control activity
- Interview business owners to understand *normal*
  - At application and business-process level

Procedural Controls
Investigation Objectives

Invest in both investigative capabilities and expertise

- Log search and correlation solutions
  - To answer “who did what…” *quickly*
- Forensic analysis solutions
  - Control for attempts to delete or otherwise hide evidence
- Multiple simple tools
  - Defense in depth
- Certification
  - So results can withstand court challenge, if necessary

Procedural Controls
Recovery Objectives

In spite of everything, an event has occurred.

Now what?

- Is it an incident?
- Procedural controls to define steps to recovery
  - Objective: first to safeguard your infrastructure
  - Objective: then to restore things back to normal
- Incident-response SOP
  - You do have one, formally documented, right?
  - Conduct drills if the business can support it

Procedural Controls
Recovery Objectives

First, stop the bleeding

- Is there more of whatever you've discovered?
- Is it designed to "blow up" if you try to disable it?
- Keep a low profile until you're sure you know what's going on

Then, eradicate

- Make forensically-acceptable copies of relevant data if you can

Next, recover

- Restore from known-uncontaminated backups
- Validate the system is really clean before returning to production
- Monitor the system for a while to make sure the risk is gone

Finally, conduct a post-mortem

- Determine what happened
- Improve defenses – they clearly are not adequate

Procedural Controls
Post-Mortem Actions

What happened? How were controls inadequate?

- Commission
  - Rogue subverted controls?
  - How did this happen? How could this happen?
- Omission
  - Controls bypassed? SOPs ignored?
  - When, where and from whom did the neglect begin and/or continue?
- Incompleteness
  - Uncontrolled risk
  - Oversight, or decision to not implement one or more controls?

Procedural Controls
Post-Mortem Actions

Explanations must be crystal-clear and brutally honest

- To repeat, **your controls were inadequate**
- The safety of your business demands that you know why
- Especially if the truth is embarrassing
  - Doubly so if it embarrasses *you*

For each instance of inadequacy, identify

- Proposal to remediate
- Resources, in dollars and people, needed to implement
- Whether all stakeholders have committed to the work
  - And when they can begin
- How long till implementation, from what start date
- Proposal on whether and how to control the risk in the meantime

Procedural Controls
Post-Mortem Actions

Have **serious** discussions with management

- Anticipate the inevitable “how could you let this happen?”
- From your post-mortem defense-improvement proposals
- Characterize the risk to the business
  - In business not technology terms
  - Compliance: regulatory or contract requirements, company policy
- Insist on clear guidance on next steps
  - Mitigate fully
  - Mitigate partially, with compensating controls
  - Formally accept the risk
- Align
  - Unwilling to follow policy? Rewrite the policy
- Remember, you should have done all this *before* the incident
  - If you don’t do it now, you **will** fail again

Reflections

Information Security is different from IT

- Security people must understand IT, but are separate from it
- No one should own both security and IT operational tasks
  - Separation of duties requires nothing less
  - Security folks are trusted insiders too

Convergence of Information and Physical Security

- They are more alike than we geeks like to admit
  - ID-badge vs. user-ID and password
  - Firewall vs. individualized building-access
  - Video vs. log records
- Phys-Sec has operated security processes far longer
  - Info-Sec can learn from Phys-Sec's process-stability
- It's all about the People, the Product, and the Data

Reflections

Ironically, preparation improves trust

- "Trust but verify" becomes trust *because* verify
  - Not about *individual* privileged user, but what a rogue someone with their access could do
  - "With great power comes great responsibility"
  - Pain from emergency recovery falls on privileged users…
  - …so prevention is very much in their interest
  - Happens faster the more management models the behavior
- Relationship can then move from adversarial to partner
  - Privileged users, who know the system best, are best positioned to identify how to run it more securely

Questions?