

Auditing Data Leaks

BRETT HESTERBERG

JUNE 7, 2011



- **Trouble at the Sheriff's Office**
- **Data Leaks – Needle in a haystack?**
- **Solve a Data Leak Mystery**
- **Hitachi IT Operations Director**
- **Summary**



One (of many) data leak examples

A database leak in Mesa County, Colorado has left the personal information of 200,000 people in jeopardy. And not just any 200,000 people—these are suspects, victims, and informants working with the sheriff's department to out other criminals.

- ars technica

- **What happened?**

- Employee copied info from DB in the form of a giant text file, assuming that the target server was secure
 - It was not secure
- File contained names, phone numbers, addresses, and Social Security numbers of numerous individuals associated with criminal investigations
- Google's Web crawler indexed the data

- **Outcome**

- Sheriff's office and FBI had to determine who could be in jeopardy
- "[W]e're talking about people's personal safety," Sheriff Stan Hilkey told the AP.

Data Leaks – Needle in a Haystack?

From a recent Data Leakage survey:

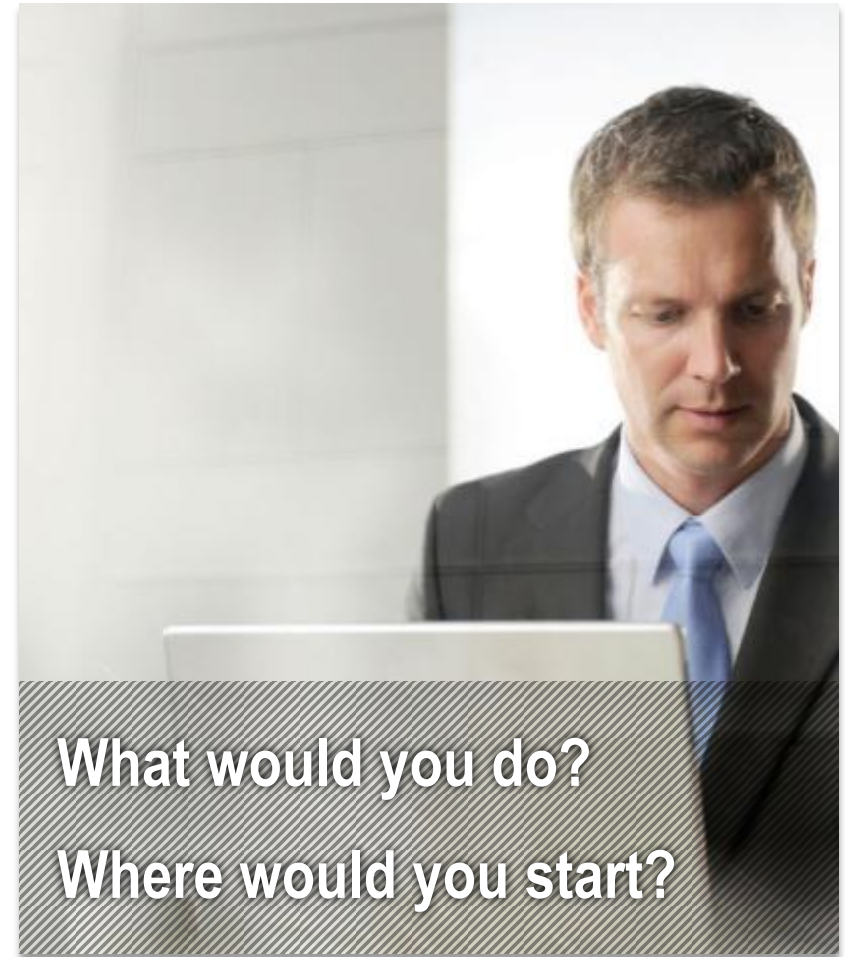
- 39% of IT professionals worldwide were more concerned about the threat from their own employees than the threat from outside hackers
- 20% of IT professionals said disgruntled employees were their biggest concern in the insider threat arena



Top concerns among IT Pros regarding data leakage:

- 1) USB devices (33% of responses)***
- 2) Email (25% of responses)***

- **You are the IT Manager at a small, publically listed company called NBI Inc.**
 - **The CFO storms into your office and tells you that @insidetrader just tweeted “NBI Q3 Net Income Per Share = \$1.14”**
 - **The information is accurate**
 - **He demands you help him find the leak**



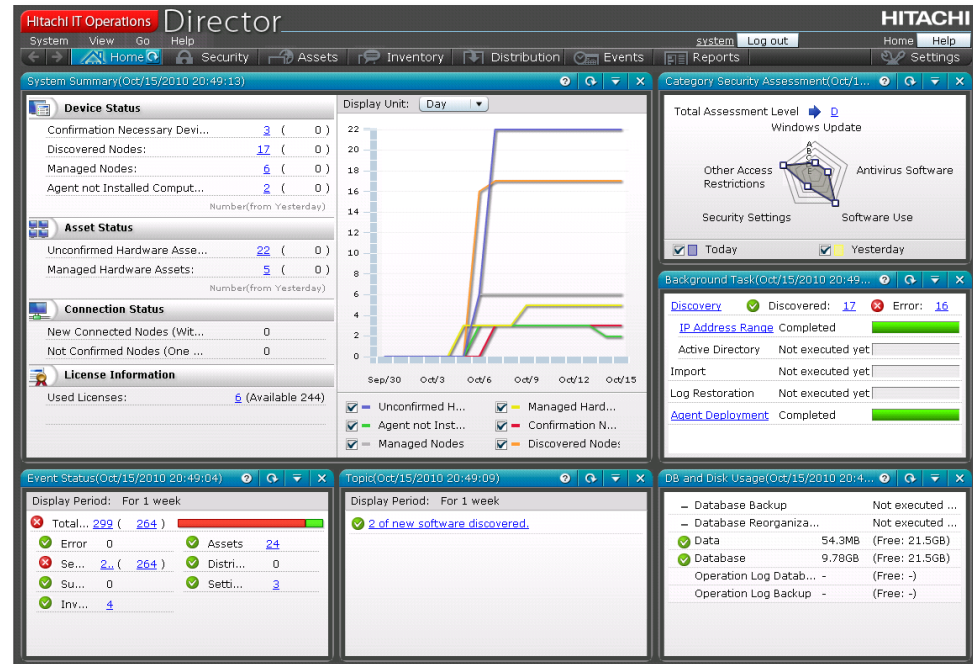
- You read @insidetrader's Tweet history and find that NBI has not previously been mentioned
- The company is small and you don't believe @insidetrader is an employee

If all else fails: Open a brokerage account and start following @insidetrader on Twitter?

Could you solve this mystery with your current tools? What is your next step?

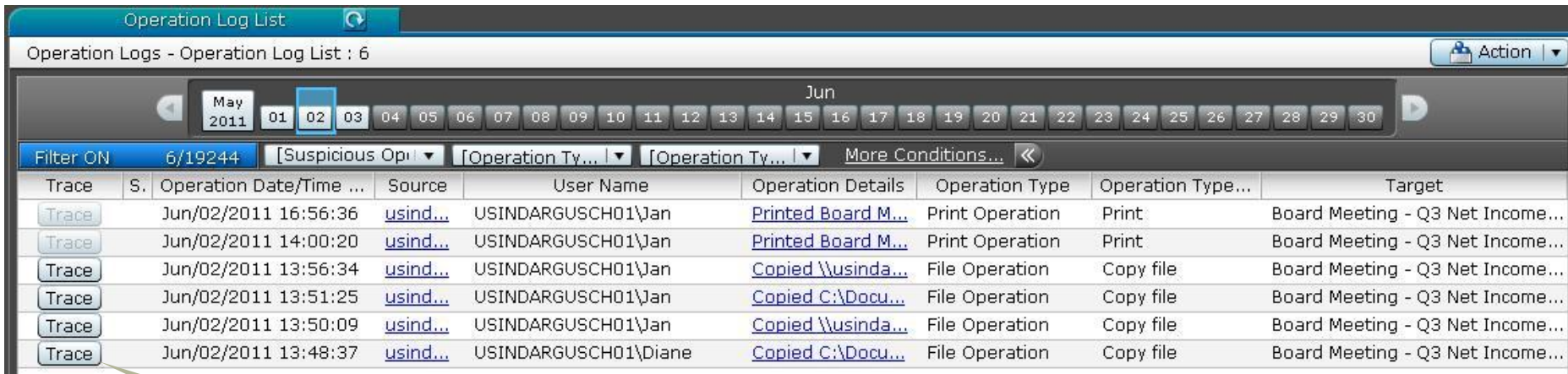
The Right Tool

- **Hitachi IT Operations Director allows you to audit the flow of information in your IT environment at a file level**



- You begin be asking the CFO for the names of relevant files that include the Q3 Net Income numbers
 - Board Meeting - Q3 Net Income.ppt
 - Oracle_export_Q3_raw.xls

- Investigate from the beginning
 - Check Director's Operation Log for the file called “Board Meeting - Q3 Net Income.ppt”



Trace	S.	Operation Date/Time ...	Source	User Name	Operation Details	Operation Type	Operation Type...	Target
Trace		Jun/02/2011 16:56:36	usind...	USINDARGUSCH01\Jan	Printed Board M...	Print Operation	Print	Board Meeting - Q3 Net Income...
Trace		Jun/02/2011 14:00:20	usind...	USINDARGUSCH01\Jan	Printed Board M...	Print Operation	Print	Board Meeting - Q3 Net Income...
Trace		Jun/02/2011 13:56:34	usind...	USINDARGUSCH01\Jan	Copied \usinda...	File Operation	Copy file	Board Meeting - Q3 Net Income...
Trace		Jun/02/2011 13:51:25	usind...	USINDARGUSCH01\Jan	Copied C:\Docu...	File Operation	Copy file	Board Meeting - Q3 Net Income...
Trace		Jun/02/2011 13:50:09	usind...	USINDARGUSCH01\Jan	Copied \usinda...	File Operation	Copy file	Board Meeting - Q3 Net Income...
Trace		Jun/02/2011 13:48:37	usind...	USINDARGUSCH01\Diane	Copied C:\Docu...	File Operation	Copy file	Board Meeting - Q3 Net Income...

Click “Trace” to see audit trail

Find the Data Leak – Trace File Operations

- Follow the flow of information using the Trace feature

Trace Operation Log

User Name: USINDARGUSCH01\Jan

Operation Type: File Operation

Operation Type (Detail): Copy file

Operation Details: Copied \\usindargusge01\c\$\Board Meeting - Q3 Net Income.ppt (Network Drive) to C:\Documents and

Original File Created Date/Time: Jun/02/2011 13:44:31

Log Tracing

Initial Operation

S...	Operation Date/Time ...	Source	User Na...	Operatio...	Operatio...	Operation ...
	Jun/02/2011 13:44:31	usindar...	USINDA...	Created...	File Ope...	Create file

Final Operation

S...	Operation Date/Time ...	Source	User Na...	Operatio...	Operatio...	Operation Typ...
	Jun/02/2011 13:56:34	usindar...	USINDA...	Copied...	File Ope...	Copy file

Trace Logs from Initial Operation to Selected Final Operation. [Export Operation Log List](#)

S...	O...	Source	User Name	Operatio...	Operatio...	Operation Type ...
J...	usind...	USINDARGUSCH01\Diane	Created...	File Ope...	Create file	
J...	usind...	USINDARGUSCH01\Diane	Change...	File Ope...	Rename file	
J...	usind...	USINDARGUSCH01\Diane	Copied...	File Ope...	Copy file	
J...	usind...	USINDARGUSCH01\Jan	Copied...	File Ope...	Copy file	
J...	usind...	USINDARGUSCH01\Jan	Copied...	File Ope...	Copy file	

[Help](#) [Close](#)

Trace Logs from Initial Operation to Selected Final Operation.

Export Operation Log List

S...	O...	Source	User Name	Operatio...	Operatio...	Operation Type ...
J...	usind...	USINDARGUSCH01\Diane	Created...	File Ope...	Create file	
J...	usind...	USINDARGUSCH01\Diane	Change...	File Ope...	Rename file	
J...	usind...	USINDARGUSCH01\Diane	Copied ...	File Ope...	Copy file	
J...	usind...	USINDARGUSCH01\Jan	Copied ...	File Ope...	Copy file	
J...	usind...	USINDARGUSCH01\Jan	Copied ...	File Ope...	Copy file	

Find the Data Leak – View Details

- View details of each file operation



Source File Information:

C:\Documents and Settings\Diane\Desktop\Board Meeting - Q3 Net Income.ppt

Source File Drive Type:

Local Disk

Destination File Information:

\\usindargusch01\C\$\Board Meeting - Q3 Net Income.ppt

Destination File Drive Type:

Network Drive

Find the Data Leak – View Details

- View details of the Print operation

The screenshot shows the 'Operation Log List' interface. At the top, there's a header bar with 'Operation Log List' and a refresh icon. Below it, a sub-header reads 'Operation Logs - Operation Log List : 6'. A navigation bar includes a calendar for May 2011 and a date range from 01 to 30. Filter options are set to 'Filter ON 6/19244', '[Suspicious Op]', '[Operation Ty...]', and '[Operation Ty...]', with a 'More Conditions...' link. The main table lists operations with columns: Trace, S., Operation Date/Time, Source, User Name, Operation Details, Operation Type, Operation Type..., and Target. The first row is highlighted, showing a print operation on Jun/02/2011 16:56:36 by user USINDARGUSCH01\Jan, targeting 'Board Meeting - Q3 Net Income...'. A 'Log Details' dialog box is open, providing more information about this specific operation.

Log Details

Operation Date/Time (Browser): Jun/02/2011 16:56:36
Operation Date/Time (Source): Jun/02/2011 19:56:36 GMT-05:00
Source: [usindargusch01.corp.hds.com](#)
User Name: USINDARGUSCH01\Jan
Operation Type: Print Operation
Operation Type (Detail): Print
Operation Details: Printed Board Meeting - Q3 Net Income - Notepad for 1 pages with \\ussccfp06v\USSCCCAN5180A.
Printed Document Name: Board Meeting - Q3 Net Income
Printer Name: \\ussccfp06v\USSCCCAN5180A
Printed Page Count: 1

Buttons: ? Help, Copy to Clipboard, Close

Click "Operation Details" for deeper information

- **After tracing operations on “Board Meeting - Q3 Net Income.ppt”**
 - Try calling Jan at desk
 - VM message says she is traveling to London this week
- **Finally Reach Jan in the UK and ask about copies of presentation**
 - She has one set with her at the hotel
 - Realizes she left the second copy at Logan Airport while waiting for her flight
- **Mystery solved**

- **Insider threat is not just the rogue employee**
- **Data leakage often results from risky behavior by employees who are unaware that their actions are unsafe**
 - **Some of this problem can be attributed to a lack of corporate policy or inadequate communication of corporate policies to employees.**
- **IT must first be able to track the flow information and find rogue data copies**
 - **Beyond tracking flow of information, IT must begin to safeguard against leaks**

INTRODUCING

IT OPERATIONS DIRECTOR



Why hitachi?



- **10th largest software company in the world***
- **Experienced in storage management and systems management software**
- **Leveraging that experience to**
 - Increase channel-driven business
 - Expand opportunities from enterprise into medium sized businesses

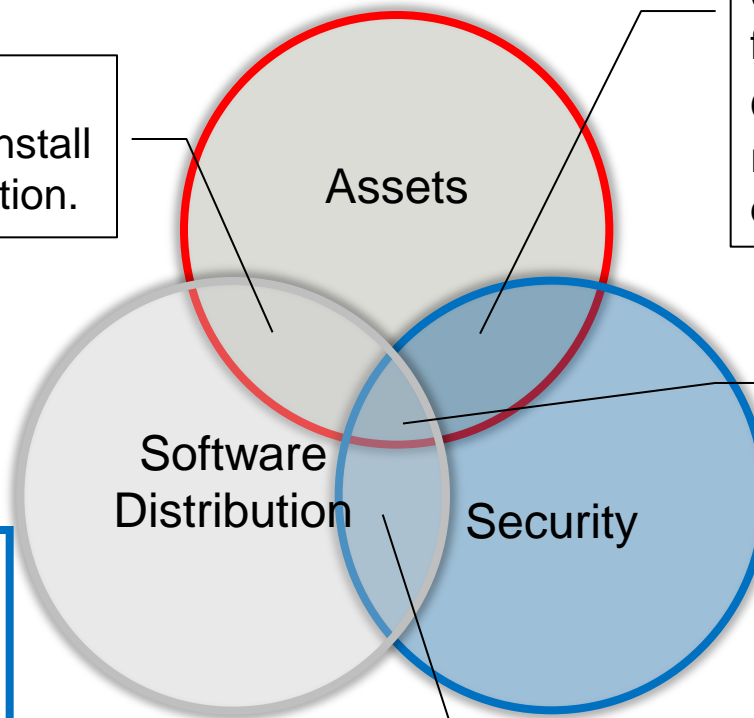
*Source: Software Magazine

What is IT Operations Director?

Hitachi IT Operations Director is an integrated solution focused on key IT infrastructure management functions - Security Management, Asset Management, and Software Distribution.

Monitor software licenses compliance and install/un-install in case of compliance violation.

By combining key functions all in one product, each will integrate with the other to provide a powerful solution in managing the client/desktop environment



Simple asset registration for USB memory.
Only allow the use of registered USB memory devices

Comprehensive dashboard and daily/weekly/monthly report.

Automatically install software and uninstall in cases where software violates the security policy.

Web-based console

Easy-to-use, intuitive interface.

The screenshot displays the Hitachi IT Operations Director web console. The interface includes a top navigation bar with tabs for System, View, Go, and Help. Below this is a main content area with several panels: Device Status, Asset Status, Connection Status, License Information, Event Status, Topic, and DB and Disk Usage. A line graph is visible in the center, showing data trends over time. A 'Category Security Assessment' panel on the right shows a radar chart for various security metrics. A 'Home - Layout Settings' dialog box is open in the foreground, allowing users to customize the layout and content of the console. The dialog box includes a 'Panel Layout' section with three grid templates and a 'Show Panels' section with a list of panels to be displayed.

Hitachi IT Operations Director

System Summary(Oct/15/2010 20:49:13)

Device Status

Confirmation Necessary Devi...	3 (0)
Discovered Nodes:	17 (0)
Managed Nodes:	6 (0)
Agent not Installed Comput...	2 (0)

Number(from Yesterday)

Asset Status

Unconfirmed Hardware Asse...	22 (0)
Managed Hardware Assets:	5 (0)

Number(from Yesterday)

Connection Status

New Connected Nodes (Wit...	0
Not Confirmed Nodes (One ...	0

License Information

Used Licenses:	6 (Available 244)
----------------	-------------------

Display Unit: Day

Category Security Assessment(Oct/15/2010 20:49:13)

Total Assessment Level

Windows Update

Other Access Restrictions

Security Settings

Antivirus Software

Software Use

Background Task(Oct/15/2010 20:49:13)

Discovery

IP Address Range

Active Directory

Import

Log Restoration

Agent Deployment

DB and Disk Usage(Oct/15/2010 20:49:13)

Database Backup

Database Reorganiza...

Data

Database

Operation Log Datab...

Operation Log Backup

Event Status(Oct/15/2010 20:49:04)

Display Period: For 1 week

Total...	299 (264)
Error	0
Se...	2 (264)
Su...	0
Inv...	4
Assets	24
Distri...	0
Setti...	3

Topic(Oct/15/2010 20:49:09)

Display Period: For 1 week

2 of new software discovered.

Home - Layout Settings

Panel Layout

Show Panels

- Home
- System Summary
- Event Status
- Background Task
- Topic
- DB and Disk Usage

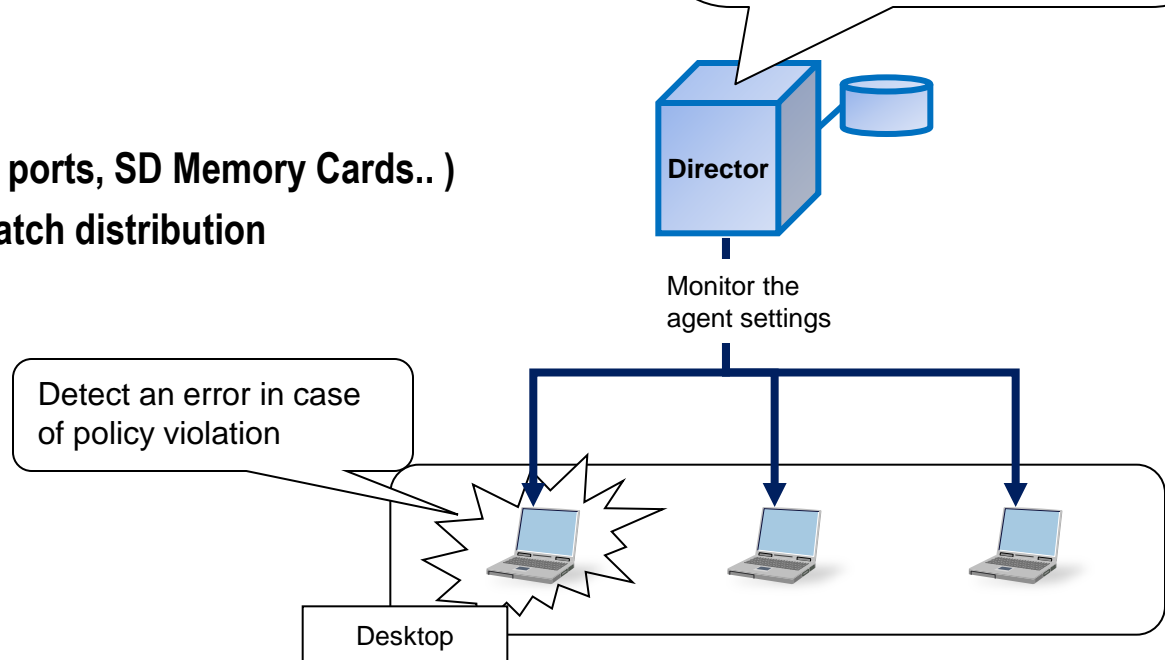
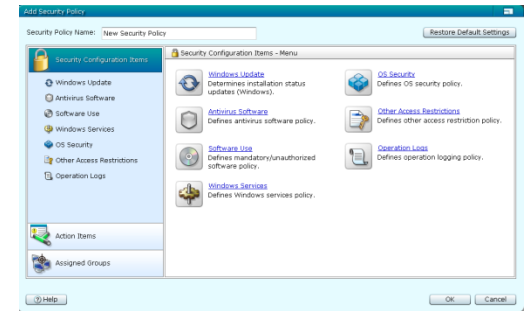
Help OK Cancel

Customize layout and content



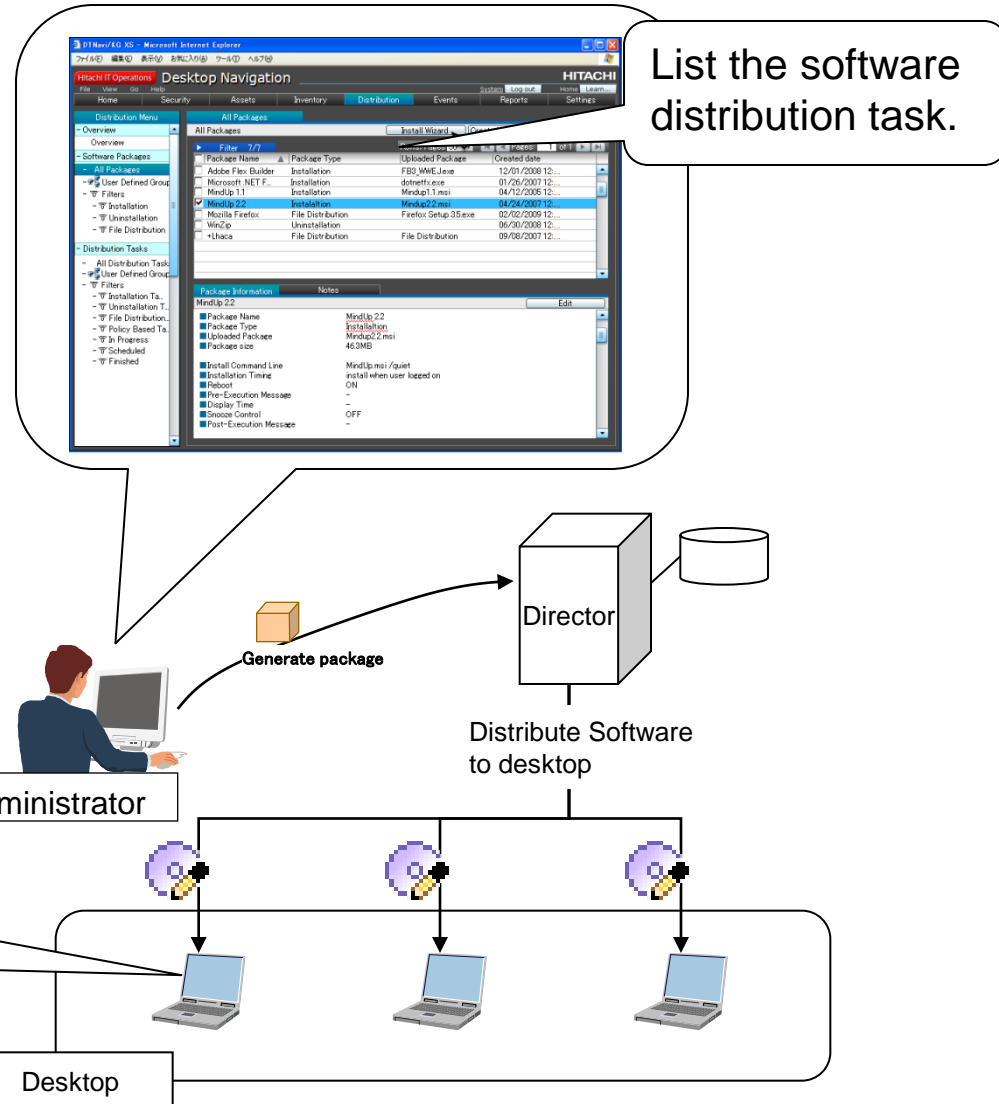
IT Roadmap
CONFERENCE & EXPO
An IDG Enterprise Event

- ## Define policies



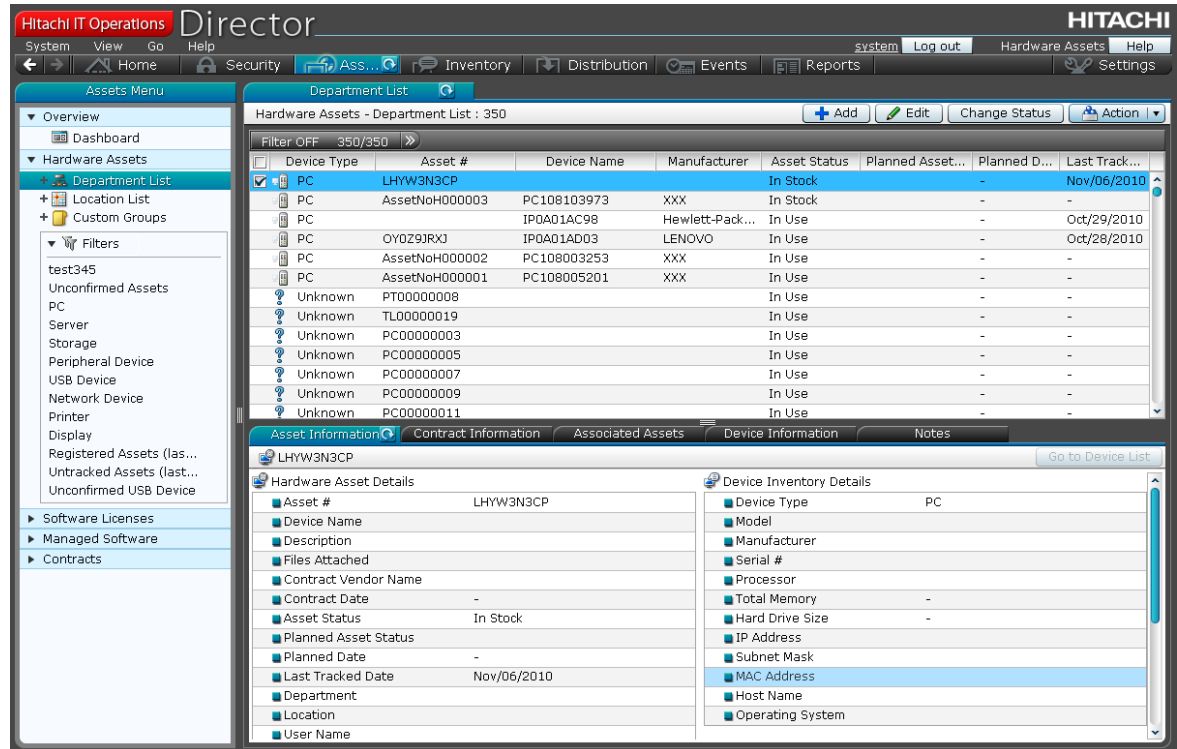
Distribution Module

- Distribution of software packages
 - Executables (MSI, EXE)
 - Scripts based (BAT)
 - Compressed packages (ZIP)
- Can be distributed on defined schedule.
(Immediately, Midnight, Morning specified date etc.)
- Can be distributed on Security Policy triggers



Assets Module

- Asset Module manages following topics.
 - Hardware Assets
 - Server
 - Desktop
 - Storage
 - Switch
 - Any other Assets
 - Software License Assets
 - Asset Contract



The screenshot displays the Hitachi IT Operations Director interface. The top navigation bar includes 'Hitachi IT Operations Director', 'System', 'View', 'Go', 'Help', 'Security', 'Ass...', 'Inventory', 'Distribution', 'Events', 'Reports', 'Log out', 'Hardware Assets', and 'Help'. The left sidebar shows the 'Assets Menu' with options like 'Overview', 'Dashboard', 'Hardware Assets', 'Department List', 'Location List', 'Custom Groups', and 'Filters'. The main content area shows a 'Department List' for '350/350' with a table of hardware assets. Below the table, the 'Asset Information' tab is selected, showing details for asset 'LHYW3N3CP'.

Device Type	Asset #	Device Name	Manufacturer	Asset Status	Planned Asset...	Planned D...	Last Track...
PC	LHYW3N3CP			In Stock	-		Nov/06/2010
PC	AssetNoH000003	PC108103973	XXX	In Stock	-		
PC		IP0A01AC98	Hewlett-Pack...	In Use	-		Oct/29/2010
PC	OY0Z9JRJ	IP0A01AD03	LENOVO	In Use	-		Oct/28/2010
PC	AssetNoH000002	PC108003253	XXX	In Use	-		
PC	AssetNoH000001	PC108005201	XXX	In Use	-		
Unknown	PT00000008			In Use	-		
Unknown	TL00000019			In Use	-		
Unknown	PC00000003			In Use	-		
Unknown	PC00000005			In Use	-		
Unknown	PC00000007			In Use	-		
Unknown	PC00000009			In Use	-		
Unknown	PC00000011			In Use	-		

Asset Information | Contract Information | Associated Assets | Device Information | Notes

Hardware Asset Details

Asset #	LHYW3N3CP
Device Name	
Description	
Files Attached	
Contract Vendor Name	
Contract Date	-
Asset Status	In Stock
Planned Asset Status	
Planned Date	-
Last Tracked Date	Nov/06/2010
Department	
Location	
User Name	

Device Inventory Details

Device Type	PC
Model	
Manufacturer	
Serial #	
Processor	
Total Memory	-
Hard Drive Size	-
IP Address	
Subnet Mask	
MAC Address	
Host Name	
Operating System	

Assets Module - Track Asset Costs

- **Contracts contain information about:**

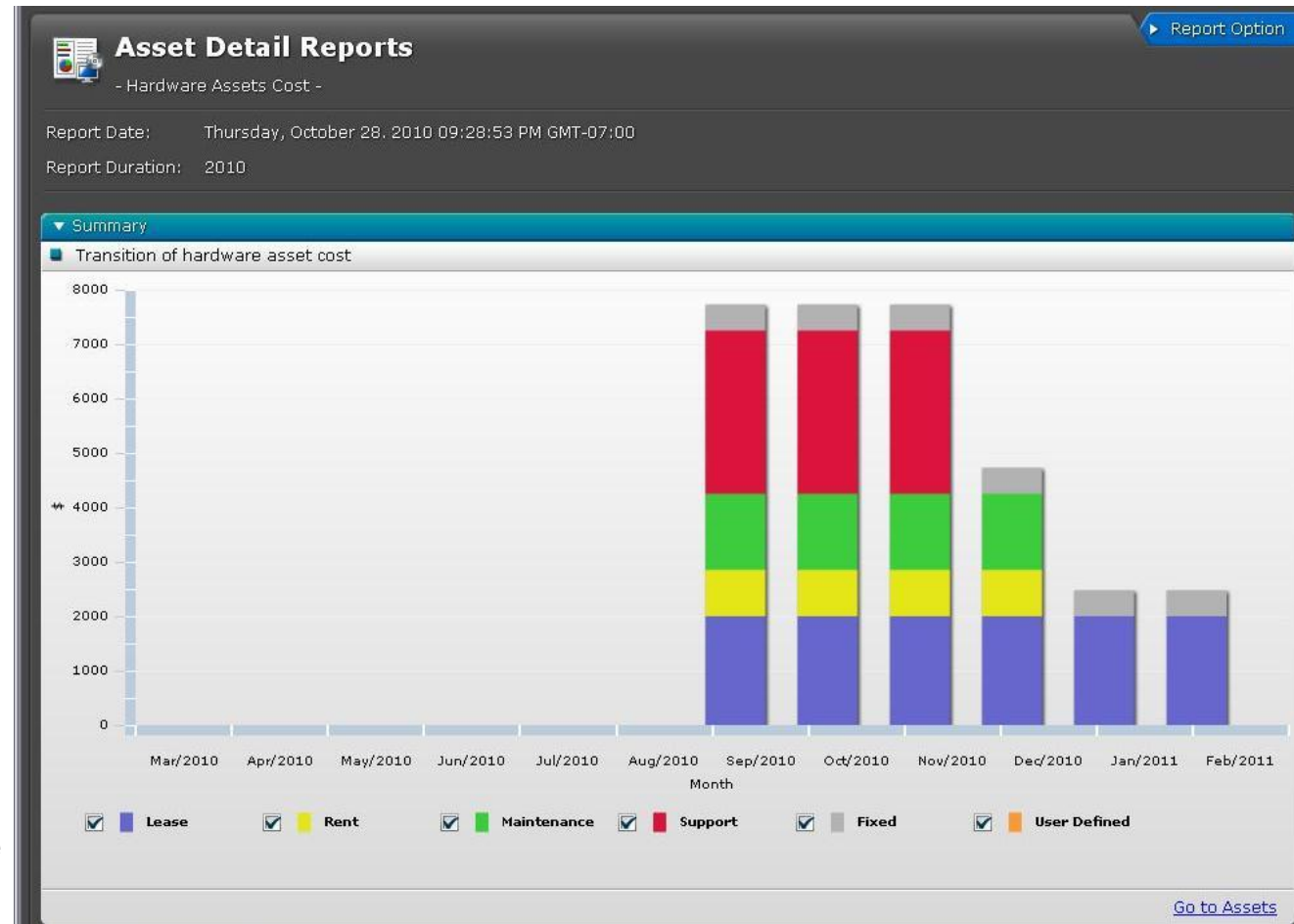
- Vendor
- Term
- Cost Structure
 - Lease
 - Rent
 - Maintenance
 - Support
 - Fixed
- Payment schedule

Can be associated with multiple assets

Hardware devices
Software licenses

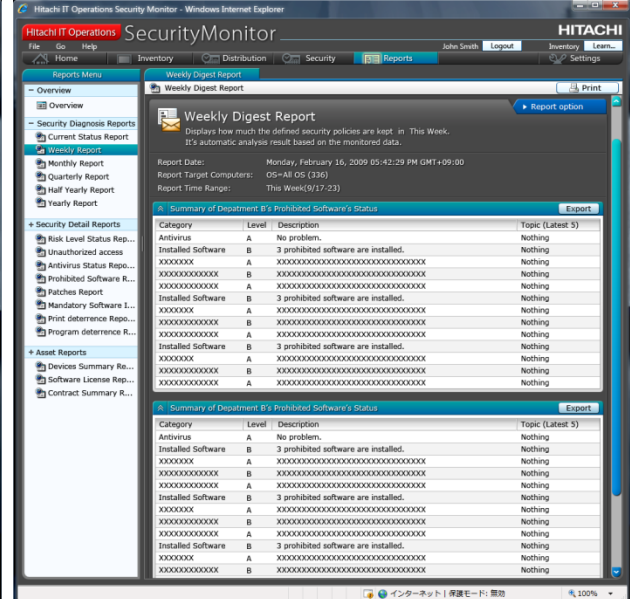
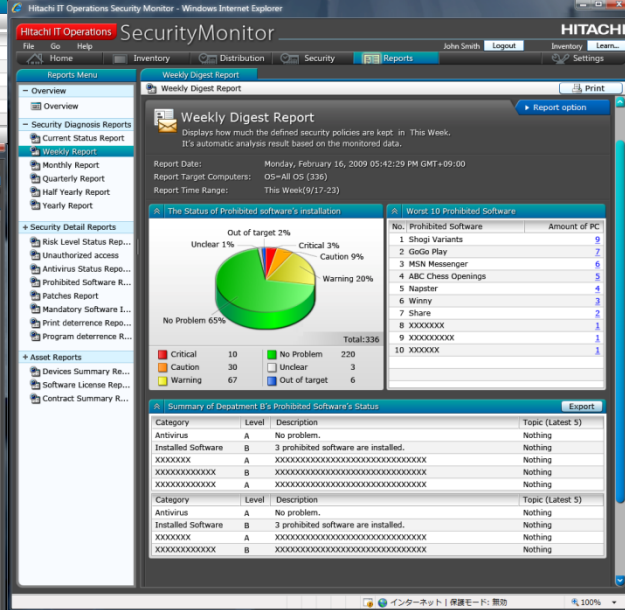
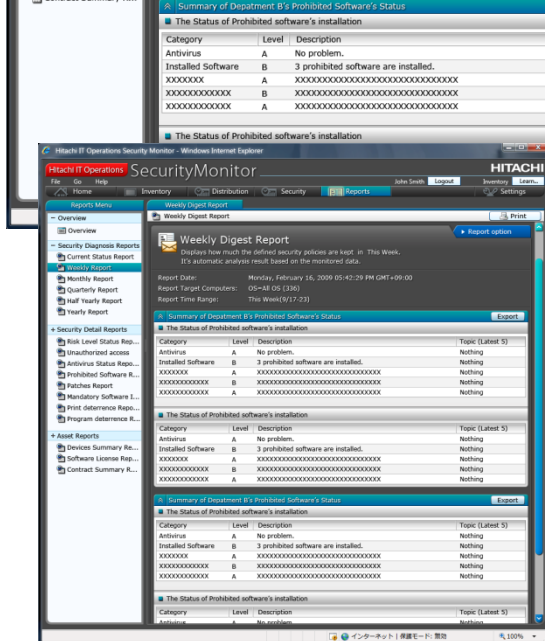
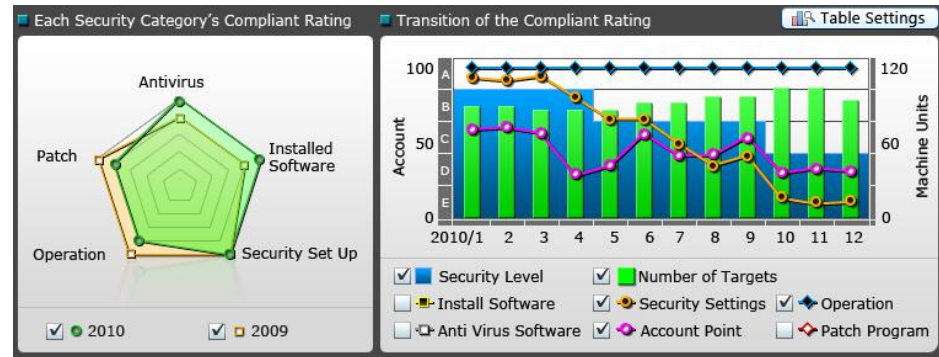
Report on:

- Trend analysis of hardware and software asset costs
- Cost structure breakdown
- Software license compliance



Reporting

Reports for Security, Assets, Software Distribution and summary for all modules.



Questions and discussion

Thank you

- **Colorado Sheriff Data Leak:**
 - <http://arstechnica.com/security/news/2010/12/informants-suspects-outed-in-accidental-database-leak.ars>
- **Data Leak stats:**
 - http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html
 - http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf