

# IS4231

# Information Security Management

## Lecture 6

### Security Management Practices

AY 2021/2022 Semester 1

**Lecturer:** Dr. YANG Lu

**Reading:** Chapter 9

# Learning Objectives

---

- ▶ List the elements of key information security management practices
  - ▶ Security employment practices
- ▶ Describe the key components of a security performance measurement program
  - ▶ Type 1: Implementation Measures
  - ▶ Type 2: Effectiveness/Efficiency Measures
  - ▶ Type 3: Impact Measures

---

# Security Employment Practices



# Hiring

---

- ▶ From an information security perspective, the hiring of employees is laden with potential security pitfalls
- ▶ The CISO, in cooperation with the CIO and relevant information security managers, should establish a dialogue with HR personnel so that InfoSec considerations become part of the hiring process



## Background checks



## Certifications



## EMPLOYMENT POLICY

### 1. PURPOSE

The purpose of this policy is to define expectations, roles and responsibilities of all HAL employees with regular to regulatory hiring and employment compliance.

### 2. SCOPE

This policy applies to all HAL employees, management, contractors, interns and volunteers. This policy address all aspects of recruitment, hiring, evaluation and termination of HAL employees and contractors. This policy describes HAL's objectives and policies regarding the maintenance of privacy and personnel information specifically including personally identifiable information (PII) and protected health information (PHI).

## Policies

### Non-Disclosure Agreement

(Confidentiality Agreement)

1. The confidential information to be disclosed by Discloser under this Agreement ("Confidential Information") can be described as and includes:

Technical and business information relating to Discloser's proprietary ideas, patentable ideas copyrights and/or trade secrets, existing and/or contemplated products and services, software, schematics, research and development, production, costs, profit and margin information, finances and financial projections, customers, clients, marketing, and current or future business plans and models, regardless of whether such information is designated as "Confidential Information" at the time of its disclosure.

In addition to the above, Confidential Information shall also include, and the Recipient shall have a duty to protect, other confidential and/or sensitive information which is (a) disclosed by Discloser in

## Covenants and agreements



### EMPLOYMENT CONTRACT

THIS AGREEMENT, made as of the 21 day of March, 2016.  
Between:  
Hierarchical Access Limited Corporation Ltd.,  
a company incorporated pursuant to the laws of the State of Georgia  
(Hereinafter referred to as "the Employer")  
- And -  
John Doe, (hereinafter referred to as "the Employee")

WHEREAS the Employee and the Employer wish to enter into an employment agreement governing the terms and conditions of employment;

THIS AGREEMENT WITNESSETH that in consideration of the premises and mutual covenants and agreements hereinafter contained, and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged by the parties hereto), it is agreed by and between the parties hereto as follows:

1. Term of Employment  
The employment of the Employee shall commence the date hereof and continue for an indefinite term until terminated in accordance with the provisions of this agreement.

## Contracts

## Figure 9-1 Hiring issues

Source: Top left: iStock.com/Hailshadow. Bottom center: iStock.com/MichaelDeLeon.

# Background Checks

---

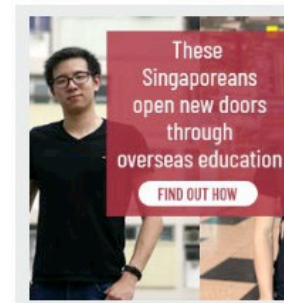
- ▶ A background check should be conducted before the organization extends an offer to any candidate, regardless of job level
- ▶ Common types include:
  - Identity
  - Education and credential
  - Previous employment verification
  - References
  - Worker's compensation history
  - Motor vehicle records
  - Drug history
  - Medical history
  - Credit history
  - Civil court history
  - Criminal court history

# Background Checks Issues

---

## ► Singapore HIV Data Leak Case, 2019

US court finds Farrera-Brochez guilty in Singapore HIV data leak case



ST VIDEOS ▶

Degrees from Vanderbilt University, a doctorate from the Sorbonne, and a teaching certificate from Kentucky state in the United States. American Mikhy Farrera Brochez, 34, had none of these, but he had forged the certificates and used them to obtain teaching positions here over a period of eight years.

# Background Checks Issues

---

## Law graduate fined S\$10,000 for doctoring NUS degree certificate, transcript to improve job prospects

*Published* 18 JANUARY, 2018 *UPDATED* 18 JANUARY, 2018

2434 Shares



SINGAPORE — Months after being called to the Bar, Jaya Anil Kumar doctored her grades for 21 modules in her degree transcript to burnish her academic performance when she applied to join the public legal service, but was not offered a job.

Three years later, the 29-year-old tried the same trick again, forging her results further for 18 modules such that she appeared to hold a Second Upper honours degree from the National University of Singapore (NUS).

Source: <https://www.todayonline.com/singapore/law-graduate-fined-s10000-doctoring-nus-degree-certificate-transcript-improve-job>



# Background Checks

Dear [REDACTED],

As part of the government's [Smart Nation initiative](#), NUS is issuing electronic (e-) degree scrolls/graduate diplomas and transcripts to our graduates with effect from 2019.

These e-documents will facilitate mobility as graduates may share them with potential employers, universities or other parties, who may access and validate them at their own time and convenience through the secured [OpenCerts platform](#) based on blockchain technology.

We are pleased to enclose an e-copy of your certificate and transcript (if applicable) with this email.

Please read the following on how to use the e-documents:

## How do I view the document?



Drag and drop the attached *OpenCerts file* into the Viewer on the [OpenCerts website](#).

## Can I save a copy?



Yes, you may download the attached *OpenCerts file* to your computer.

If you had a Singapore Identity Card or a Foreign Identification Number (FIN) when you were studying at NUS, then a copy of the file has also been deposited into the **Skills Passport** of your individual [MySkillsFuture](#) account. [Click here](#) (FAQ Q3) for more information. Once logged in, you may **link your account to a social media account** for easy retrieval in future.

## How do I share the document?



Email the *OpenCerts file* and the [OpenCerts website link](#) to your intended recipient.

Inform the recipient to drop the *OpenCerts file* into the viewer at the [OpenCerts website](#) to view the document.

For more information, you may like to visit our website [here](#).


Should you have any questions, please send an email to [transcript@nus.edu.sg](mailto:transcript@nus.edu.sg). Thank you.

With best wishes

SHAW Lay Pheng (Ms)  
Registrar  
National University of Singapore

# Personnel Security Practices

---

- ▶ There are various ways of monitoring and controlling employees to minimize their opportunities to misuse information – *Insider Threat*
- ▶ Separation of duties
  - ▶ Also known as segregation of duties
  - ▶ Work is divided up. Each team member performs only his or her portion of the task sequence
  - ▶  Control the odds of collusion - separation of duties main objective is to prevent conflict of interest
- ▶ Two-man control
  - ▶ Also known as dual control - dual control main objective is to minimise errors
  - ▶ It requires that two individuals to work together to complete. In some cases, review and approve each other's work before the task is considered complete



finance domain will usually champion such ideas since they handle massive amount of sensitive data

- opening vault need both key (person and employee)

- user updating particulars need 2 person to approve the update

# Examples:

---

## ▶ Separation of duties

### ▶ Software development

#### ▶ developing vs. testing

### ▶ Data backup

#### ▶ data backup vs. mounts and dismounts the physical media

## ▶ Two man in control

### ▶ Data center security

#### ▶ Monitor and limit access to server racks

#### ▶ “It requires that two cards with authorized access to the rack be scanned within ten seconds of one another in order for a server rack door to be opened.”

- E.g., Identocard Access Control



# Examples:

---

## ***NSA Implements 'Two-Man Rule' to Prevent Future Leaks***

In the wake of the Edward Snowden leak, the National Security Agency (NSA) has put in place a "two-man rule" that requires two people to be present for the transfer of sensitive information.

"NSA has instituted a two-person rule for systems administrators who have the highest privileges," an NSA spokesperson said via email.

The news was first reported by the Associated Press, which spoke to NSA chief Keith Alexander on the sidelines of the Aspen Security Forum in Colorado.

Alexander told the news service that the NSA is currently testing out this two-person rule within the agency, and would roll it out at the Pentagon and other intelligence agencies at a later date. One item on the agenda is coming up with rules for sites that currently only have one system admin, he told the AP.

Source: <https://www.pcmag.com/news/nsa-implements-two-man-rule-to-prevent-future-leaks>

# Personnel Security Practices (cont.)

---

- ▶ Need to know and least privilege
  - ▶ Need to know
    - ▶ The principle of limiting users' access privileges to only the specific information required to perform their assigned tasks.
  - ▶ Least privilege
    - ▶ The principle that ensures no unnecessary access to data exists by regulating members so that they can perform only the minimum data manipulation necessary
    - ▶ It implies **need-to-know.**

need to know focuses on the data access  
least privileged focuses on the rights

# Personnel Security Practices (cont.)

---

## ▶ Job rotation

- ▶ It requires that every employee be able to perform the work of at least one other employee
- ▶ Cross train employees
- ▶ If that approach is not feasible, an alternative is *task rotation*, in which all critical tasks can be performed by multiple individuals
- ▶ For similar reasons, each employee should be required to take a *mandatory vacation*, of at least one week per year
- ▶ This policy gives the organization a chance to perform a detailed review of everyone's work



# Minnesota Office of the State Auditor

Rebecca Otto



[About Our Office](#) | [Latest News](#) | [Reports & Data](#) | [For Local Officials](#) | [Auditing](#) | [Investigations](#) | [Forms](#) | [Contact Us](#)

Google Custom Search



## Mandatory Vacations

Public entities should consider a mandatory vacation policy for employees – especially those with financial responsibilities. When an employee never takes a day off from work, it may be a red flag for fraud. Employees who engage in fraud may resist taking a vacation, fearing that someone else doing their job in their absence may discover the irregularities.

For a mandatory vacation to be effective as a fraud deterrent and detection tool, someone else must be cross-trained in the bookkeeping and cash functions and must perform the work during the mandated vacation.

Date this Avoiding Pitfall was most recently published: 05/25/2018

[Privacy Policy](#) | [Accessibility Information](#) | © 2018 Office of the Minnesota State Auditor

# Termination Issues

---

- ▶ When an employee leaves an organization, the following tasks must be performed:
  - ▶ The former employee's access to the organization's systems must be disabled
  - ▶ The former employee must return all removable media, technology, and data
  - ▶ The former employee's hard drives must be secured
  - ▶ File cabinet locks must be changed
  - ▶ Office door locks must be changed
  - ▶ The former employee's keycard access must be revoked
  - ▶ The former employee's personal effects must be removed from the premises
  - ▶ The former employee should be escorted from the premises, once keys, keycards, and other business property have been turned over



- However - in practice it will be difficult to ensure that such regulations will be followed by the employee since they would not be able to have information of where the employee went afterwards
- Usually these cases are hard to detect and only detectable on an ad hoc basis

## Termination Issues (cont.)

- ▶ In addition to performing these tasks, many organizations conduct an **exit interview** to remind the employee of any contractual obligations, such as nondisclosure agreements, and to obtain feedback on the employee's tenure in the organization
- ▶ **Not-to-compete or non-compete clause**
  - ▶ Prevent them from working for a direct competitor within a specified time frame
    - ▶ A few months to several years
- ▶ **Garden Leave**
  - ▶ A way to restrict the flow of proprietary information when an employee leaves to join a competitor
  - ▶ Buffer time
- ▶ **Non-Disclosure Agreement**

Garden Leave - company will still be paid by company  
vs  
Non-Compete - a promise after leaving the company

# Garden Leave

---

## **BHP Billiton hires new global IT chief, ditches CIO title**

Mining giant BHP Billiton has hired a former General Motors executive into its new top IT role, replacing global chief information officer Chris Crozier, whose title has been retired following his departure.

Crozier is understood to have left the role he filled for six years last month after being promoted to a vice president position, but very shortly after departed the organisation and is currently on gardening leave.

Source: <https://www.itnews.com.au/news/bhp-billiton-hires-new-global-it-chief-ditches-cio-title-410404#:~:text=Diane%20Jurgens%20takes%20over%20after,been%20retired%20following%20his%20departure.>

---

# Performance Measurement in InfoSec Management

# InfoSec Performance Management

---

- ▶ Information security performance management is the process of *designing, implementing and managing* the use of the collected data elements (called measures or metrics) to determine the effectiveness of the overall security program
- ▶ Performance measurements (or measures) are data points or computed trends that may indicate the effectiveness of security countermeasures or controls—*technical and managerial*—as implemented in the organization

# Four Benefits of Using Measures

---

1. Increase accountability
2. Improve information security effectiveness
3. Demonstrate compliance
4. Provide quantifiable inputs for resource allocation decisions

# What Should Be Communicated?

---

- ▶ Information for security stakeholders and other people involved in performance measurement (5W1H)
  - ▶ Why should these statistics be collected?
    - ▶ Objective
  - ▶ What specific data will be collected?
    - ▶ Concept
  - ▶ When will these statistics be collected?
    - ▶ Situation
  - ▶ Where (at what point in the function's process) will these statistics be collected?
    - ▶ Business practice
  - ▶ Who will collect these statistics?
    - ▶ People
  - ▶ How will these statistics be collected?
    - ▶ Method

# InfoSec Performance Management (cont.)

---

- ▶ Organizations use three types of measurements:
  - ▶ Type I: Those that determine the effectiveness of the execution of InfoSec policy (like ISSPs)
    - ▶ Implementation measures, used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures
      - E.g., the percentage of information systems with password policies configured as required
      - E.g., the percentage of servers within a system with a standard configuration
      - At first, the results of these measures might be less than 100 percent. However, as the information security programs and its associated policies and procedures mature, results should reach and remain at 100 percent

# InfoSec Performance Management (cont.)

---

- ▶ Organizations use three types of measurements:
  - ▶ Type 2: Those that determine the effectiveness and/or efficiency of the delivery of information security services
    - ▶ Effectiveness/Efficiency Measures
    - ▶ Effectiveness: the robustness of the result itself
    - ▶ Efficiency: the timeliness of the result



# InfoSec Performance Management (cont.)

---

- ▶ Organizations use three types of measurements:
  - ▶ Type 3: Those that assess the impact of an incident or other security event on the organization or its mission
    - ▶ Impact measures
      - Cost savings produced by information security program
      - Costs incurred by responding to attacks and breaches
      - Level of public trust in your organization gained or maintained by the information security program

# Factors to Consider When Devising Measures

---

- ▶ According to *NIST SP 800-55 RI - Performance Measurement Guide for Information Security*, the following factors must be considered during development and implementation of an information security performance management program
  - ▶ They must be quantifiable (percentages, averages, and numbers)
  - ▶ Data that supports the measures needs to be readily obtainable
  - ▶ Only repeatable information security processes should be considered for measurement
  - ▶ Measures must be useful for tracking performance and directing resources

# Measures Development & Selection

---

- ▶ Specifying information security measures
  - ▶ One of the critical tasks in the measurement process is to assess and quantify what will be measured
  - ▶ Must identify, assess and quantify the measures that characterize the target
  - ▶ It is critical (but difficult) to get the right measures from the outset
    - ▶ Cyclical reviews will expose shortcomings in wrongly specified or inadequate measures
  - ▶ A lot of variation

# Measures Development & Selection (cont.)

---

- ▶ **Establish performance targets**
  - ▶ So that you can define what success means in the security program
  - ▶ Implementation measures typically target 100% completion of specific tasks
  - ▶ Performance targets for effectiveness/efficiency much more complex
    - ▶ Measures may not be quantifiable, so must be stated in terms of qualitative, reasoned descriptions of what constitutes success

# Performance Measurement Template and Instructions

**Table 9-1** Performance Measurements Template and Instructions

Field	Data
Measurement ID	The unique identifier used to measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source. It should be meaningful to the source and/or use of the measurement.
Goal	Statement of strategic goal and/or InfoSec goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and InfoSec goals can be included. For example, InfoSec goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific InfoSec goal extracted from agency documentation, or identify an InfoSec program goal that would contribute to the selected strategic goal.
Measurement	Statement of measurement. Identify precisely the numeric element to be measured. Start with one of percentage, number, frequency, average, or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Any related security controls providing supporting data should be identified. If the measures are applicable to a specific FIPS 199 impact level (high, moderate, or low), provide that means of evaluation.
Measurement type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.

(continues)

# Performance Measurement Template and Instructions (cont.)

**Table 9-1** Performance Measurements Template and Instructions (*continued*)

Field	Data
Implementation evidence	<p>Use of implementation evidence to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure.</p> <ol style="list-style-type: none"><li>1. For manual data collection, identify questions and data elements that would provide data inputs necessary to calculate measure's formula, qualify measure for acceptance, and validate provided information.</li><li>2. For each question or query, list status security control number from NIST SP 800-53 that provides information, if applicable.</li><li>3. If measure is applicable to a specific FIPS 199 impact level, questions should state impact level.</li><li>4. For automated data collection, identify data elements that would be required for formula, qualify measure for acceptance, and validate information provided.</li></ol>
Frequency	<p>Indication of how often the data is collected and analyzed, and how often the data is reported.</p> <p>State the frequency of data collection based on a rate of change in a particular security control that is being evaluated. State the frequency of data reporting based on external reporting requirements and internal customer preferences.</p>
Responsible parties	<p>Indication of the following key stakeholders:</p> <ul style="list-style-type: none"><li>• Information owner: Identify organizational component, an individual who owns required pieces of information.</li><li>• Information collector: Identify the organizational component and individual responsible for collecting the data. If possible, the information collector should be a different person from the information owner or even a representative of a different organizational unit, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.</li><li>• Information customer: Identify the organizational component and individual who will receive the data.</li></ul>
Data source	<p>Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.</p>
Reporting format	<p>Indication of how the measure will be reported, such as pie charts, line charts, bar graphs, or other format. State the type of format or provide a sample.</p>



# Performance Measurement Example

**Table 9-2** Performance Measurement Example

Field	Example Data
Measurement ID	Security training coverage
Goal	Strategic goal: Ensure a high-quality workforce supported by modern and secure infrastructure and operational capabilities. InfoSec goal: Ensure that organization personnel are adequately trained to carry out their assigned InfoSec-related duties and responsibilities.
Measurement	The percentage of InfoSec personnel who have received security training.
Measure type	Implementation
Formula	Number of InfoSec personnel who have completed security training within the past year divided by the total number of InfoSec personnel, then multiplied by 100
Target	100 percent
Implementation evidence	<ol style="list-style-type: none"> <li>1. Are significant security responsibilities defined with qualifications criteria and documented in policy? Yes/No</li> <li>2. Are records kept regarding which employees have significant security responsibilities? Yes/No</li> <li>3. How many employees in your department have significant security responsibilities?</li> <li>4. Are training records maintained? Yes/No</li> <li>5. How many of those with significant security responsibilities have received the required training?</li> <li>6. If all personnel have not received training, document all reasons that apply: <ol style="list-style-type: none"> <li>a. Insufficient funding</li> <li>b. Insufficient time</li> <li>c. Courses unavailable</li> <li>d. Employee not registered</li> <li>e. Other (specify)</li> </ol> </li> </ol>
Frequency	Collected as training is delivered Reported annually
Responsible parties	Information owner: training division Information collector: training division Information customer: CIO
Data source	Training and awareness tracking records
Reporting format	Pie chart illustrating the percentage of security personnel who have received training versus those who have not received training. If performance is below target, pie chart illustrating causes of performance falling short of targets.

# Examples of Possible Security Performance Measures

---

- ▶ Percentage of the organization's information systems budget devoted to information security
- ▶ Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
- ▶ Percentage of remote access points used to gain unauthorized access
- ▶ Percentage of information systems personnel that have received security training
- ▶ Average frequency of audit records review and analysis for inappropriate activity
- ▶ Percentage of new systems that have completed certification and accreditation prior to their implementation
- ▶ Percentage approved and implemented configuration changes identified in the latest automated baseline configuration
- ▶ Percentage of information systems that have conducted annual contingency plan testing
- ▶ Percentage of users with access to shared accounts
- ▶ Percentage of incidents reported within required time frame per applicable incident category
- ▶ Percentage of system components that undergo maintenance in accordance with formal maintenance schedules



# Examples of Possible Security Performance Measures (cont.)

---

- ▶ Percentage of media that passes sanitization procedures testing
- ▶ Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets
- ▶ Percentage of employees who are authorized access to information systems only after they sign an acknowledgment that they have read and understood the appropriate policies
- ▶ Percentage of individual screened before being granted access to organizational information and information systems
- ▶ Percentage of vulnerabilities remediated within organization- specified time frames
- ▶ Percentage of system and service acquisition contracts that include security requirements and/or specifications
- ▶ Percentage of mobile computers and devices that perform all cryptographic operations using organizationally specified cryptographic modules operating in approved modes of operations
- ▶ Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated

# Reporting InfoSec Performance Measurements

---

- ▶ In most cases, simply listing the measurements collected does not adequately convey their meaning
- ▶ In addition, you must make decisions about how to present correlated metrics
- ▶ The CISO must also consider to whom the results of the performance measures program should be disseminated, and how they should be delivered

# Reporting InfoSec Performance Measurements

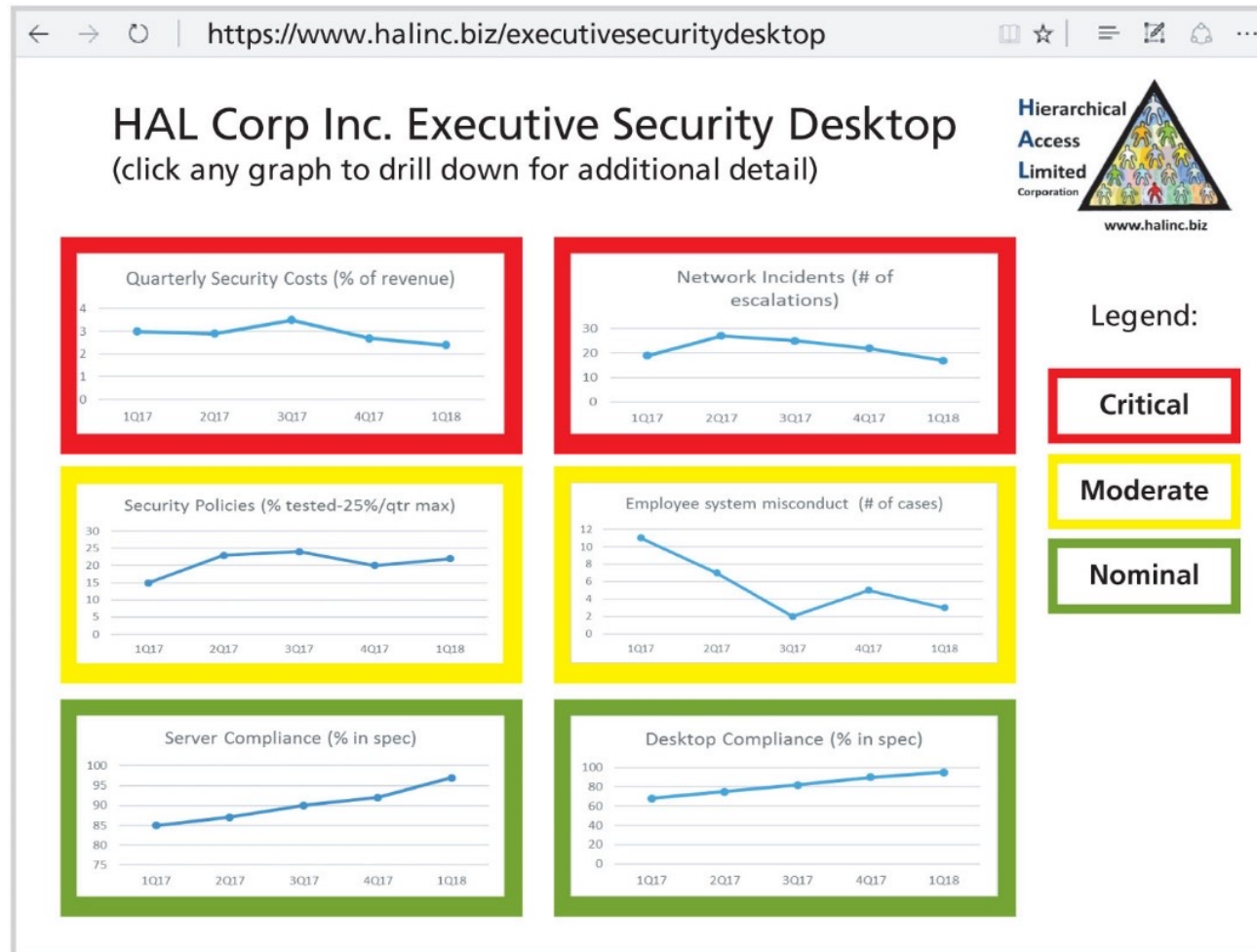


Figure 9-5 Security dashboard

# Next week

---

- ▶ **L7 Security Management Models**