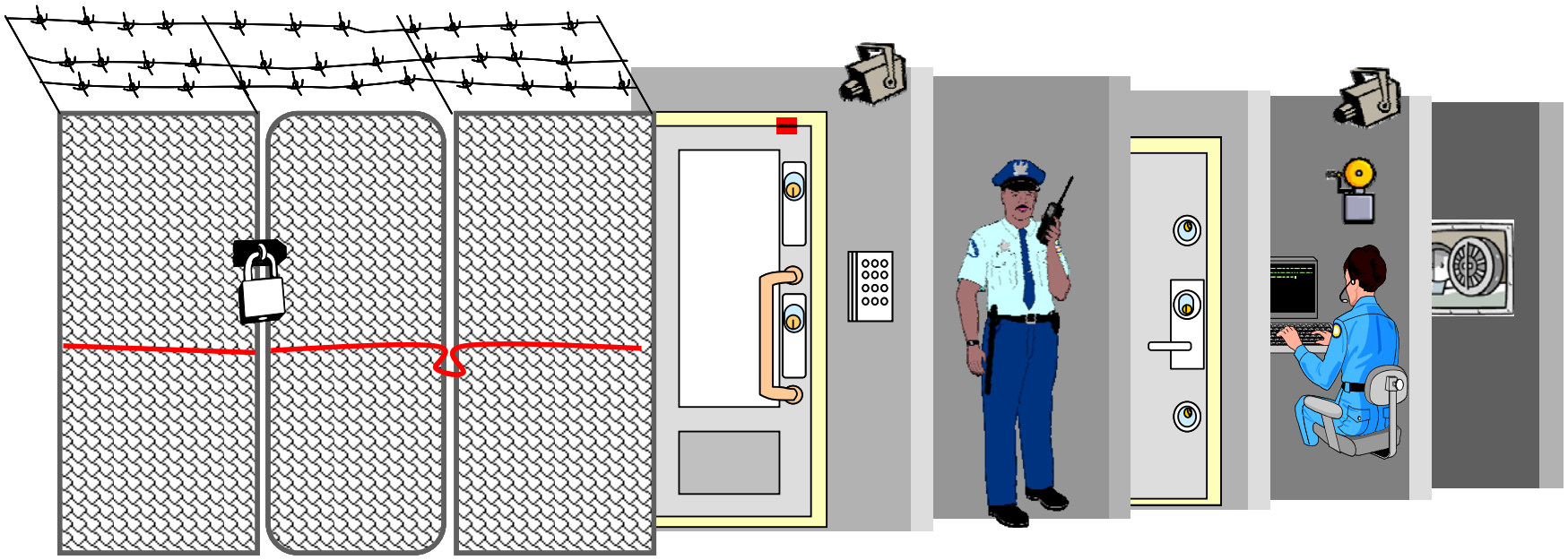
MANAGING RISK

The insider threat to biocontainment facilities

Mitigation through organizational security

Ronald Barø, Dr. Morten Mærli, Alexander F. Christiansen and Dr. Stephen McAdam
21 October 2008

Common misperception of security



Security is much more than Guns, Guards and Gates

-“Security is fundamentally not a technology problem- it's a people problem”.

-(Bruce Schneier, Februar 2008)

Background

MANAGING RISK

- The most likely security threat to any biological containment facility
- Relatively little research / studies into the insider threat with respect to biological containment facilities

What is the insider threat?

MANAGING RISK

- The insider threat comes from trusted individual(s) that steal, distribute, sabotage, destroy, or release a dangerous biological agent, or other high consequence assets like sensitive information.

Preconditions for insider betrayal

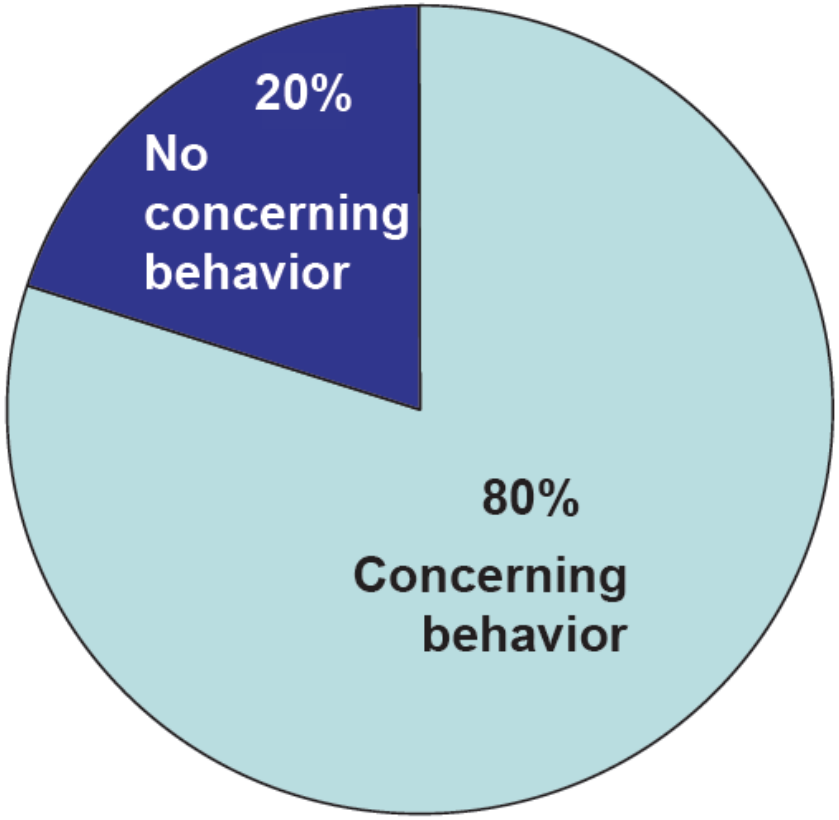
MANAGING RISK

- The following conditions are often required before an employee carries out a serious betrayal of trust:
  - ✓ An opportunity to commit the crime
  - ✓ A motive or need to be satisfied by the crime
  - ✓ An ability to overcome natural inhibitions to criminal behavior
  - ✓ A trigger that sets the betrayal in motion

PERSEREC Findings

MANAGING RISK

- A negative work-related event triggered most of the insiders' actions.
- 80% of th …viour of a security concern i …ut their activities.
- 57% of ir …bilities in applicatic
- 43% of ir …he time of the incident.



*Source: D …nter (PERSEREC)

Acquiring Biological Agents

MANAGING RISK

Table 4: Acquisition of biological agents

Type	Terrorist	Criminal	Other/ Uncertain	Total Instances
Legitimate supplier	1	9	1	11
Theft	1	3	0	4
Self-manufactured	1	4	1	6
Natural source	2	4	0	6
Unknown	3	3	0	6
Total instances	8	23	2	33

Note: This table reflects the predominant method of acquisition; some individuals or groups acquired agent through multiple paths.

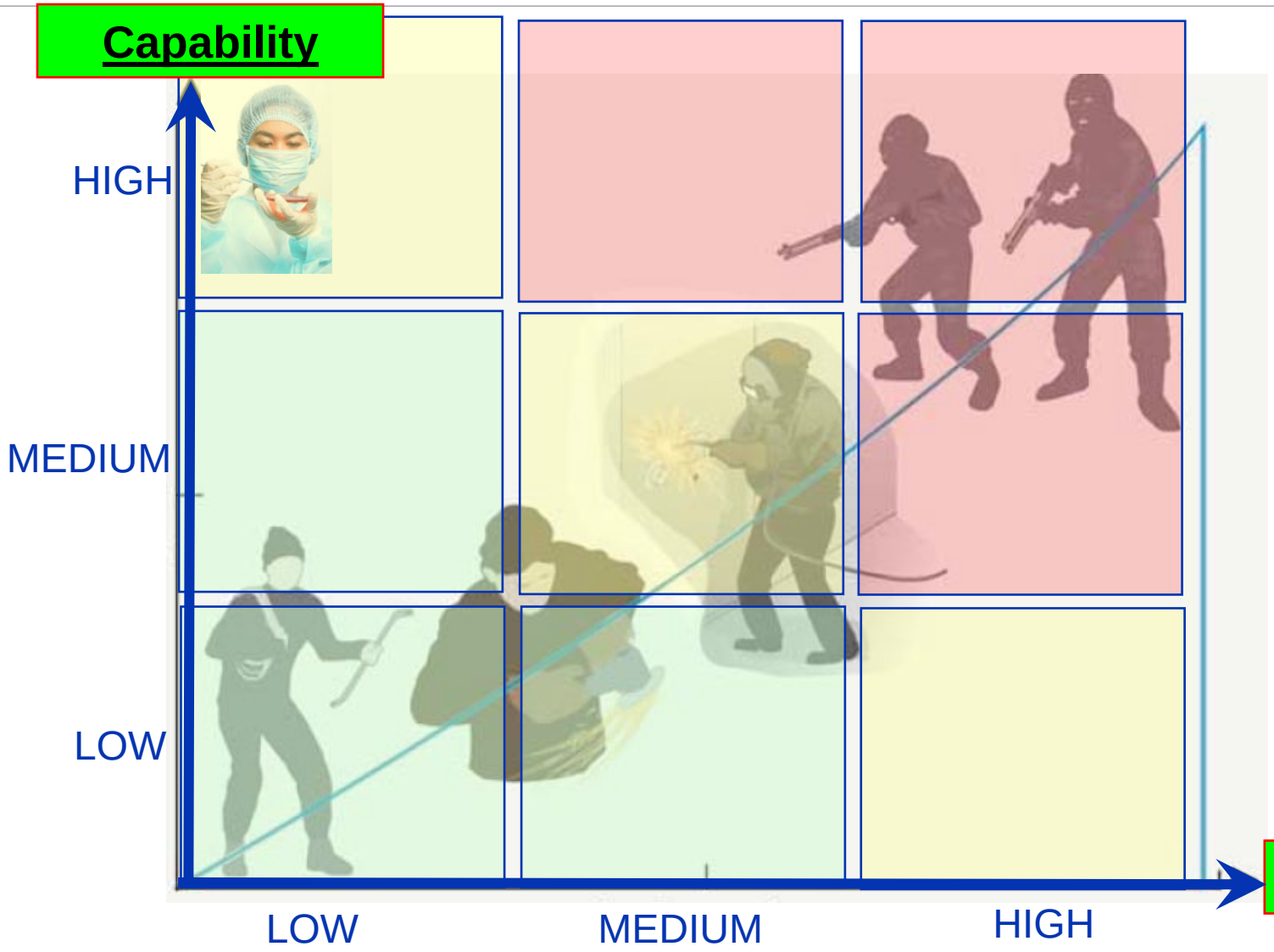
- 11 of the 33 cases involving non-state actors - obtained biological agents or toxins from legitimate suppliers (data from 1900 to 2000)

  All thefts involved people who had legitimate access to the facilities where the biological agents were kept

***Source: Bioterrorism and Biocrimes; The Illicit Use of Biological Agents Since 1900 - W. Seth Carus**

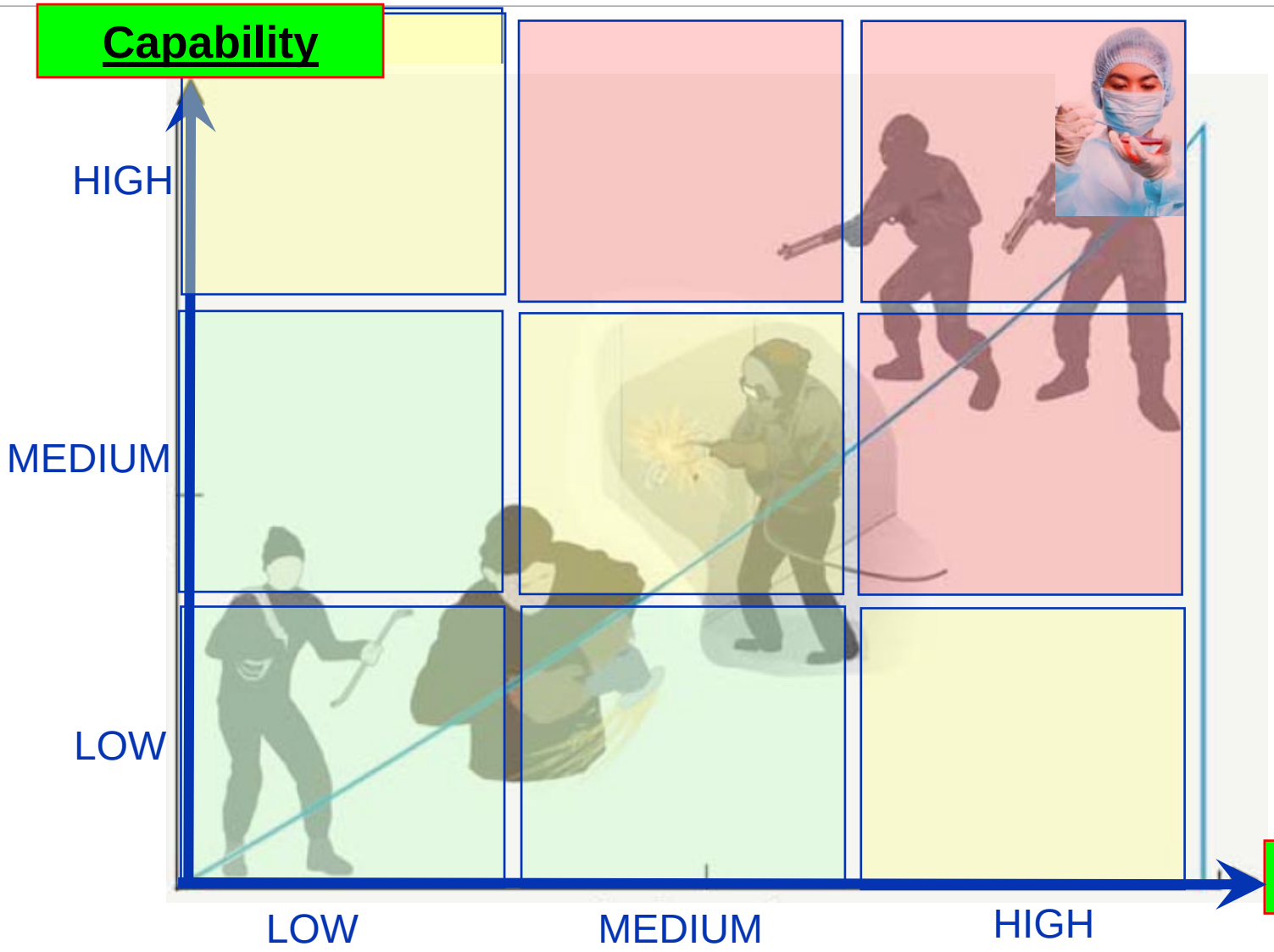
External/internal adversaries

MANAGING RISK



External/internal adversaries

MANAGING RISK



Insider pre-attack behavior

MANAGING RISK

- Previous incidents have shown
  - Insiders acted in a concerning manner in the workplace prior to the event
  - Most insiders planned their activities in advance
  - In many cases, others had information about their intentions, plans, and/or activities
  - Many insiders communicated negative sentiments to others, and even made threats of harm

➢ *Organizations should document reports of problematic behavior and develop procedures to respond to such reports*

Recognition of behavior, not stereotypes

MANAGING RISK

- No demographic “profile” of insiders
  - ages range from late teens to retirement
  - both men and women
  - at all levels: technicians, managers, executives, current / past and temporary employees, contractors

➢ Security awareness training needs to focus on behavior, not on stereotypical characteristics

➢ Behaviors that should be a cause for concern include:
  - threats against the organization
  - statements that damage could be done
  - attempts to obtain access to restricted areas through trickery or exploitation of trust

Examples of behavioural precursors

MANAGING RISK

- Drug/alcohol abuse
- Conflicts (co-workers, supervisor)
- Aggressive or violent behaviour
- Mood swings over time
- Turning more and more introvert
- Poor performance or apathetic behaviour
- Excessive money spending
- Frequently absent with no apparent reason
- Unusual interest in information outside job scope
- Unusual work hours

U.S Secret Service and CERT Insider Threat Study 2002

What is organizational security?

MANAGING RISK

- How the organization deals with security – from a human perspective
- Leadership and management
- Policies, standards, procedures
- Organizational culture
- Human Resources (HR)
- Communication
- Training and security awareness

Mitigation through organizational security

MANAGING RISK

- Executive commitment to biosecurity – top down process
- Recruiting and vetting – get the right people onboard
- Policies and procedures reinforced by education and controls
- Security awareness training with focus on behavior, not on stereotypical characteristics.
  - *Conduct activities to promote deterrence, greater possibility for detection and guard against the potential threat from the insider*

Mitigation through organizational security

MANAGING RISK

- There is a delicate balance between rigid security systems and productivity
- Enforce separation of activities
- Proactive access controls based on need
- Protect of “whistleblowers”
- To recognize behavioural change, we need to know what is a person’s typical behaviour

Not necessarily expensive

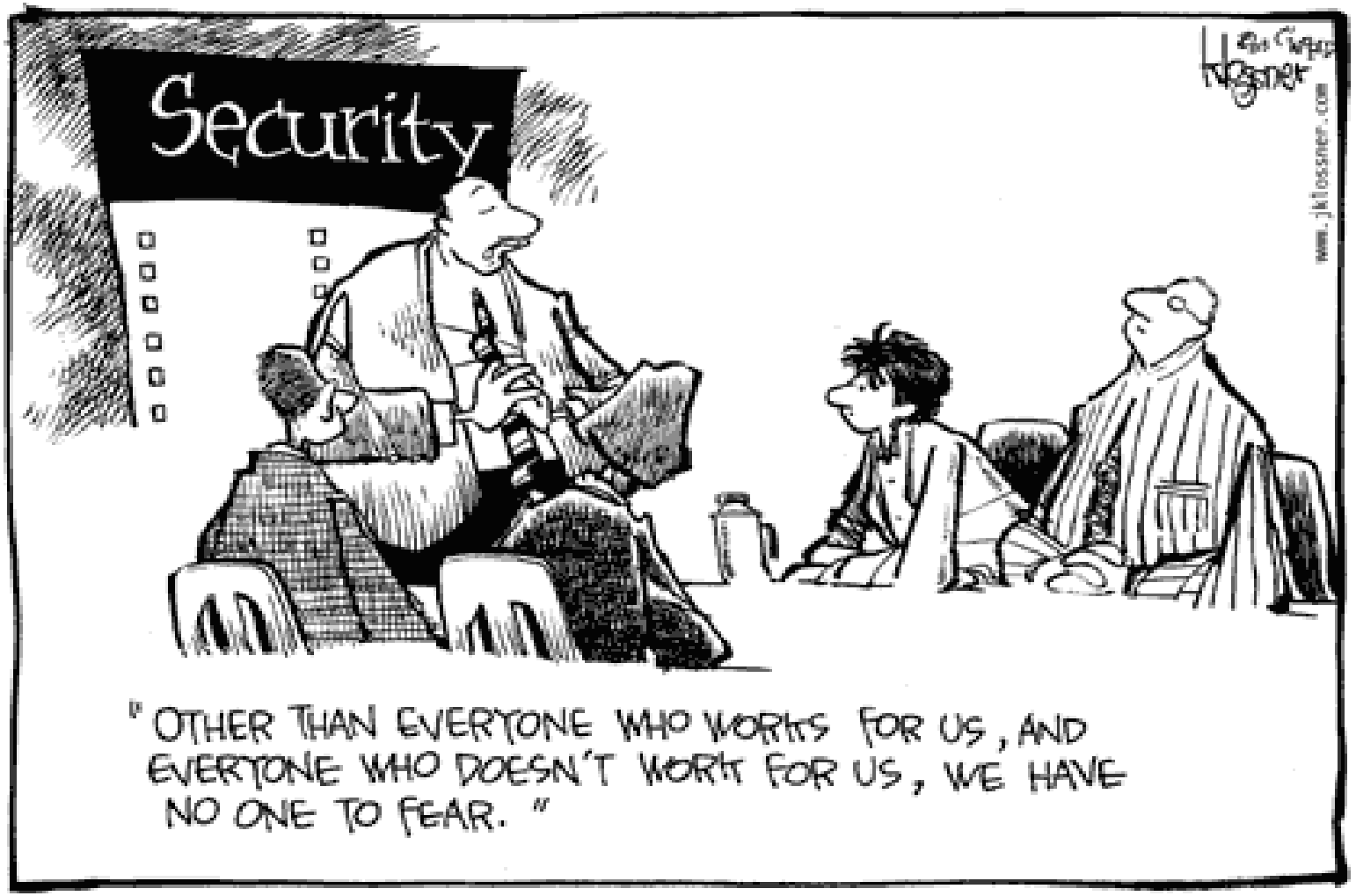
MANAGING RISK

- First rate management – know and care about your colleagues
- Organizational security is a process, not a product
- Emphasize, define and prioritize the desired organizational culture
- Implement processes to promote responsibility- regardless of position in the organization
- Organizational security can be effective without significant capital investment
- **Working with organizational security = changing mindsets**

Security awareness - not paranoia

MANAGING RISK

- It is essential to encourage and promote a climate of trust, versus one of apprehension, oppression, paranoia and distrust



Conclusions

MANAGING RISK

- Executive commitment to biosecurity is vital to mitigate the insider threat
- To identify and stop the insider threat, we must focus on human behavior and not just stereotypes
- Organizational security is the key strategy in mitigating the insider threat
- The first line of defense: colleagues and managers

www.dnv.com