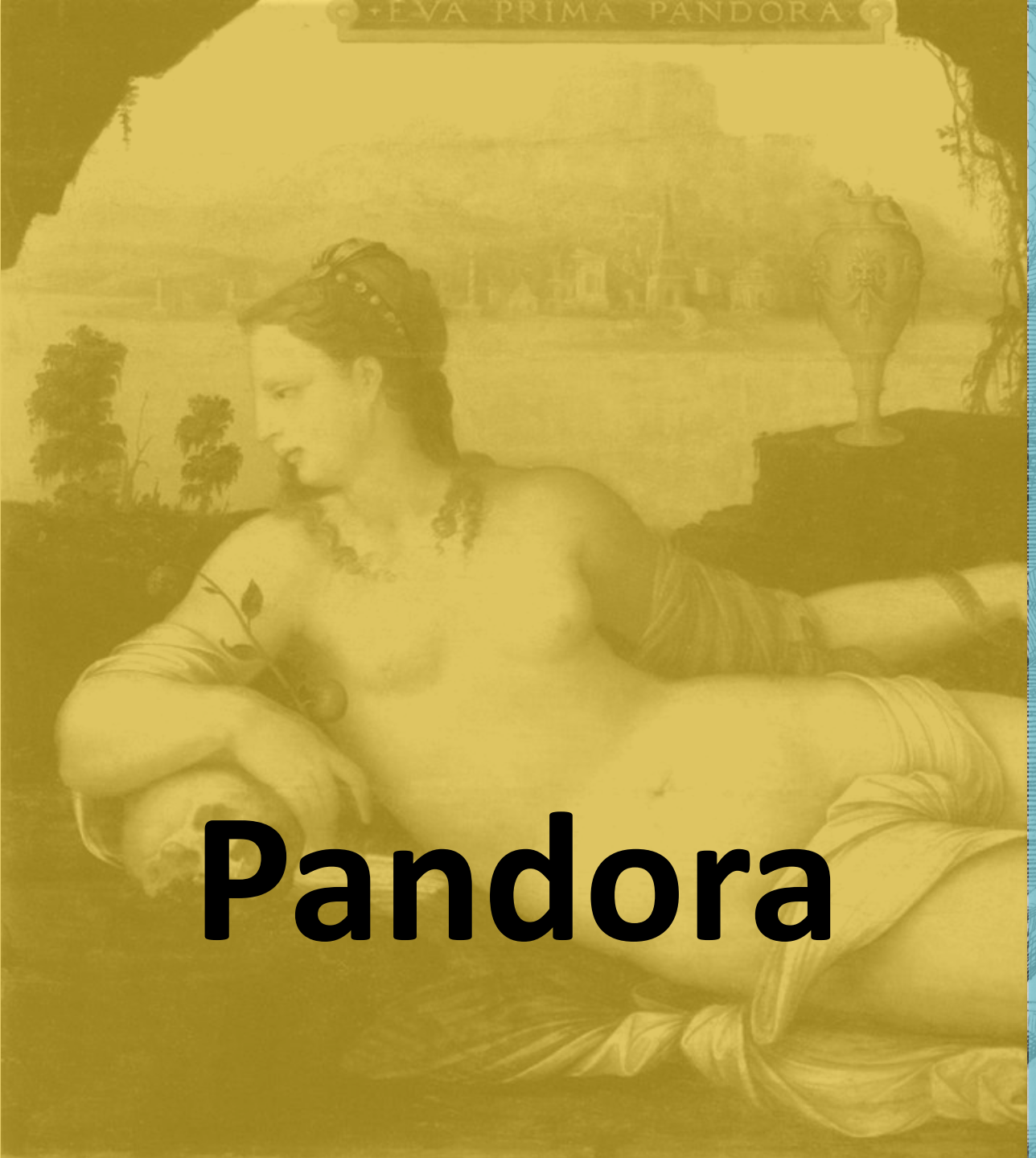
RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CXO-T06

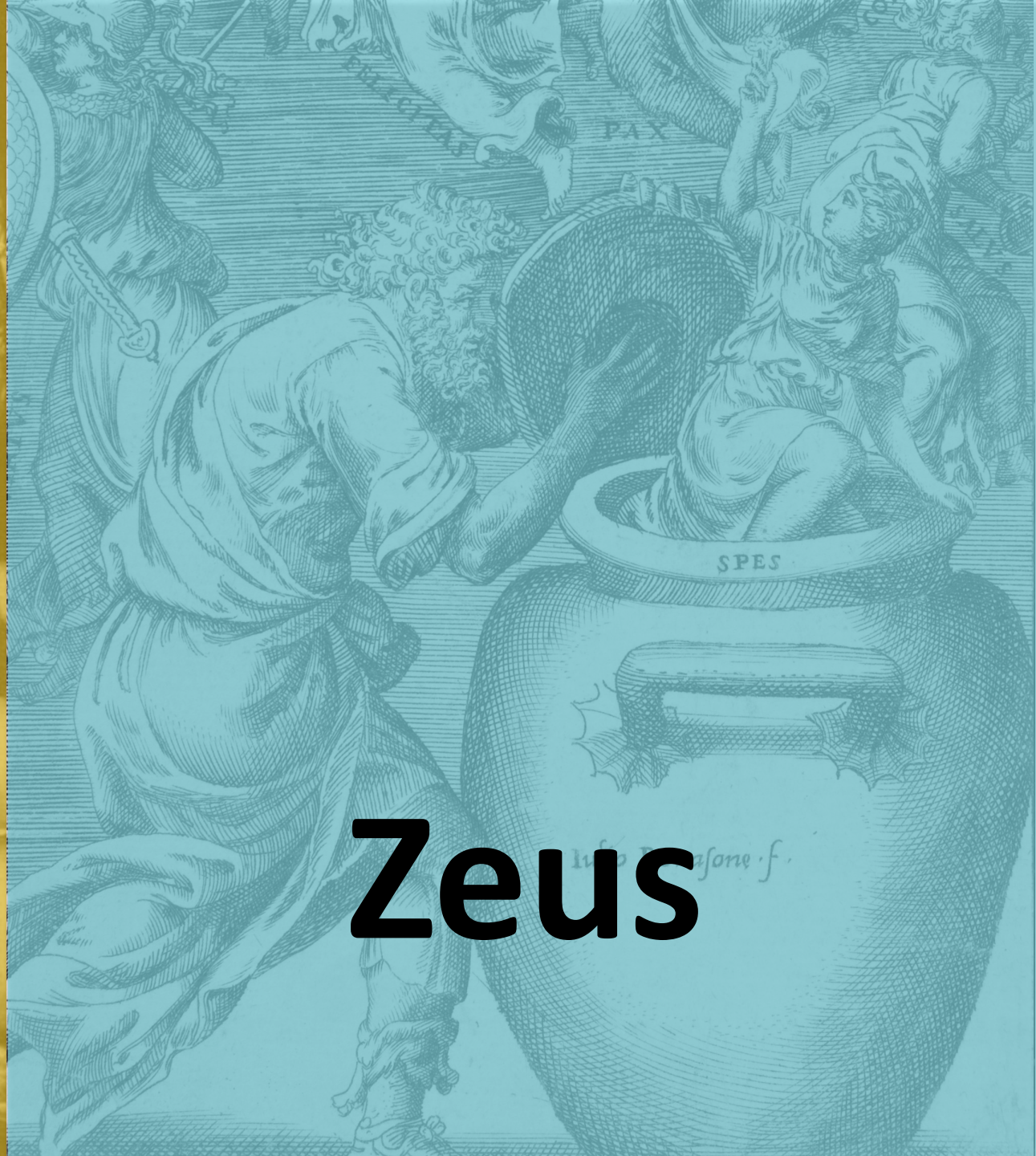
Expense in Depth: Managing Your Total Cost of Controls

Malcolm Harkins

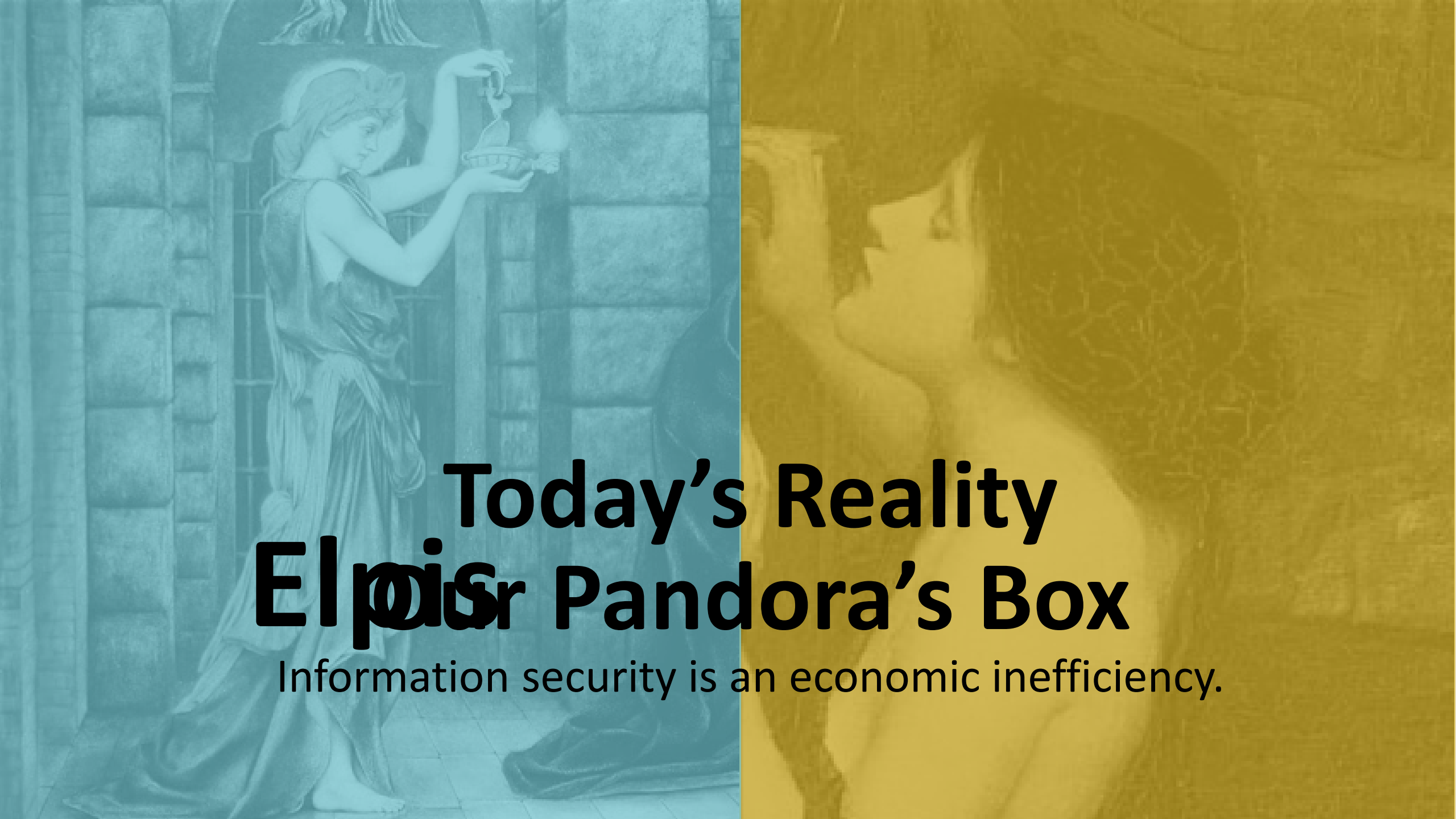
VP Chief Security & Trust Officer
Cylance®



Pandora



Zeus

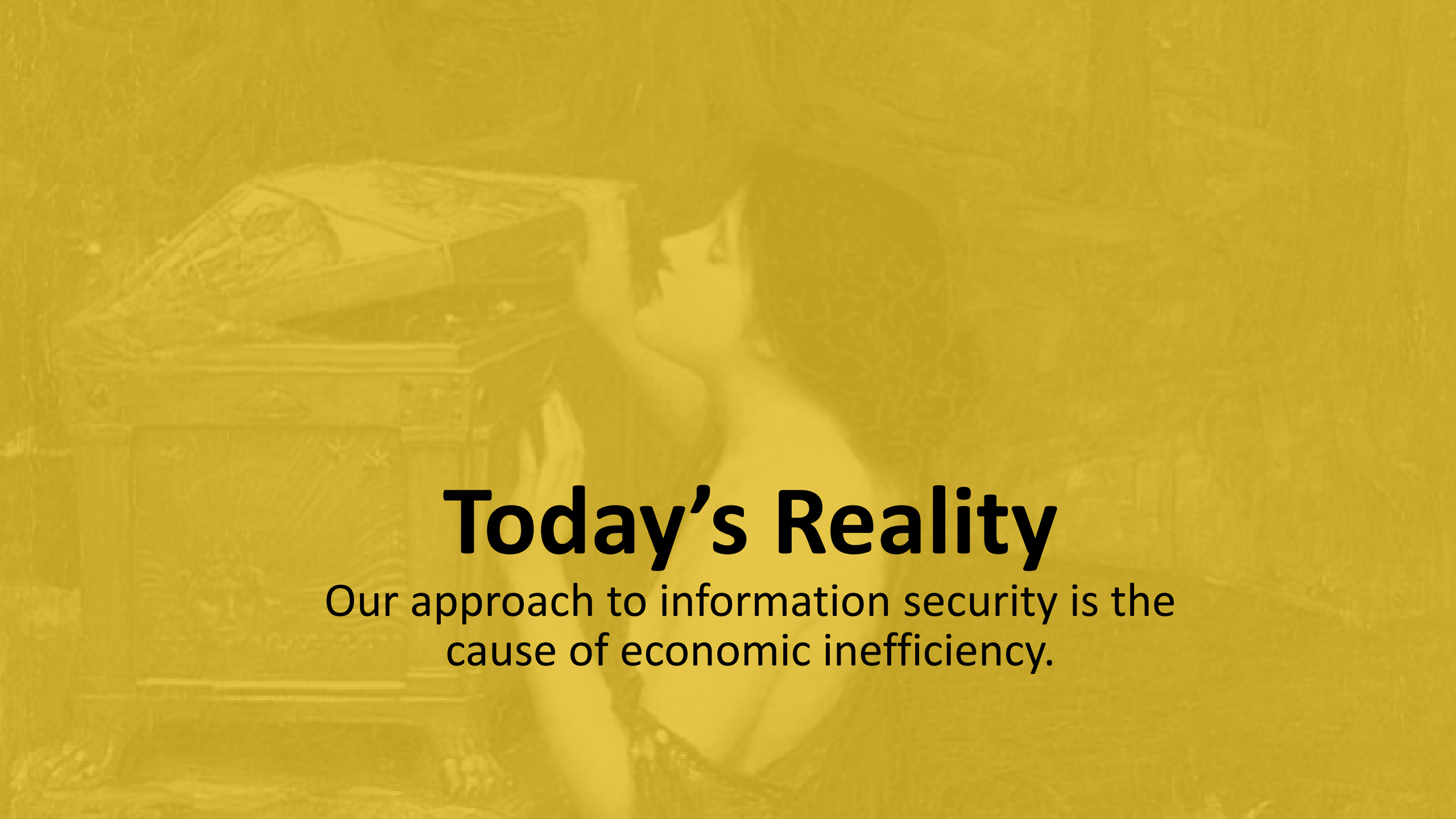


Today's Reality
Elpois or Pandora's Box

Information security is an economic inefficiency.

What Is Economic Efficiency?

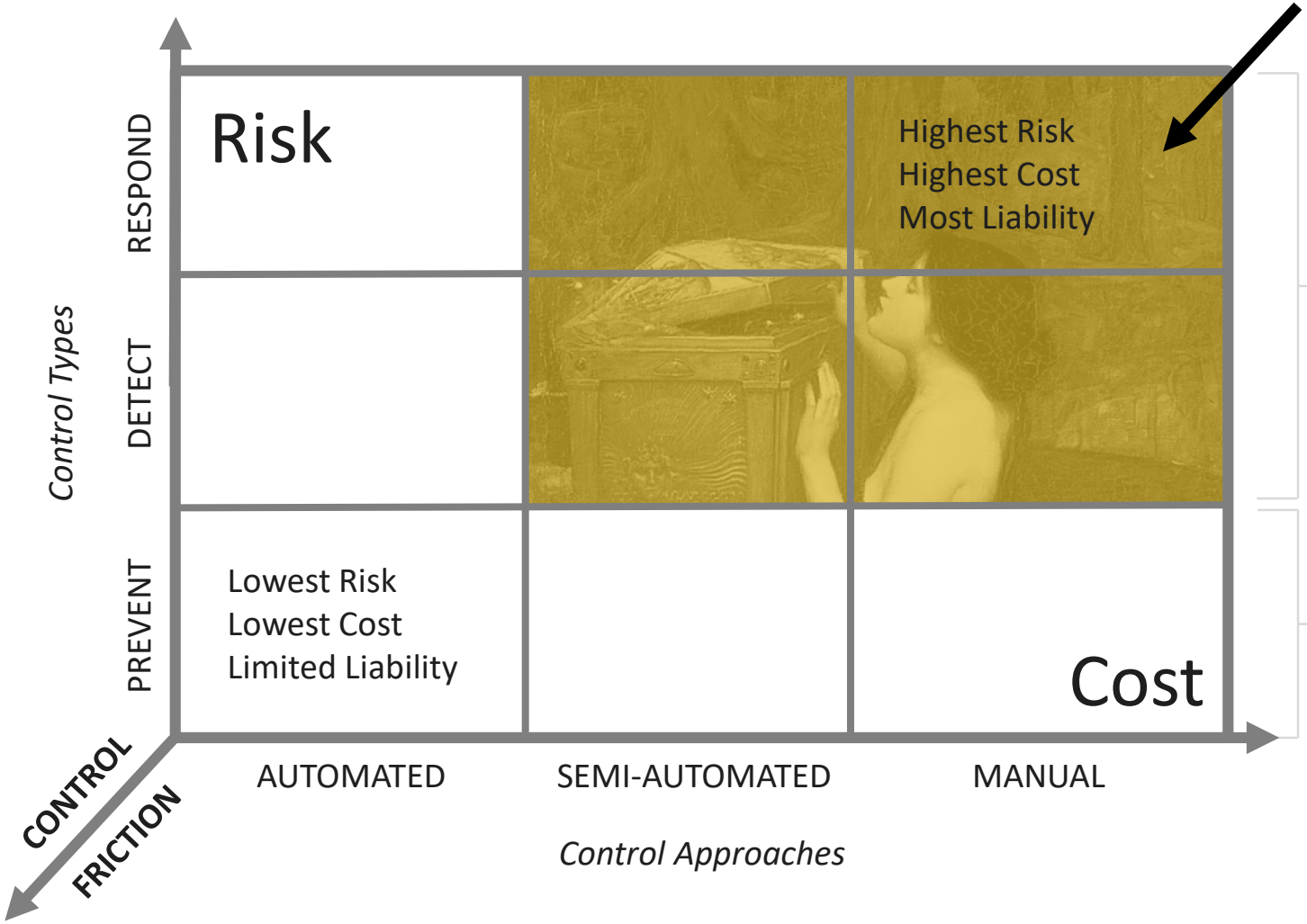
- Economic efficiency implies an economic state in which **every resource is optimally allocated to serve** each individual or entity in the best way **while minimizing waste** and inefficiency.
- The **ideal state** is related to the **welfare of the population** as a whole with peak efficiency also resulting in the **highest level of welfare possible** based on the resources available.



Today's Reality

Our approach to information security is the cause of economic inefficiency.

9 Box of Controls



Pandora's Box

Where most of the industry is focused

Focus is on minimizing damage – only variables are time to detect and time to contain

Focus is on minimizing vulnerability and potential for harm

Source: Managing Risk and Information Security 2nd edition Malcolm Harkins

What is Expense in Depth?

A culture of controls that focuses on adding additional controls to make up for the short comings of key controls that failed…

Is the Control

a risk prevention?

executed manually?

understandable?

scalable?

verifiable?

sustainable?

scoped appropriately?

timely?

mandatory?

measurable?

repeatable?

Control Design Score

Strong: control is designed properly to mitigate risk

Insufficient: control is not designed to mitigate the risk sufficiently (only partially/slightly reduces the risk, doesn't mitigate it)

Flawed: not designed properly to mitigate risk

Control Design Review Actions

If a control is insufficient or flawed

- **Redesign it:** so that it is strong
- **Remove it:** stop wasting money and time with a “false sense of control”

Total Cost

- **An economic measure that sums all expenses** paid to produce a product, purchase an investment, or acquire a piece of equipment including **not only the initial cash outlay** but also all the other expenses associated with operations over a period of time. **It includes the addition of all costs- direct and indirect.**
- **It measures the total fixed, variable, and overhead expenses** associated with producing a good.
- This is a **fundamental concept for business owners and executives** because it allows them to track the combined costs of their operations.

Total Cost of Controls

Obvious Direct Cash Buckets

- AV replacement
- Security operations
- Hunting team
- Investigations
- Legal
- Help desk calls
  - Performance complaints
  - Infection related issues
- IT operations costs
  - IT emergency response
  - Infrastructure costs
  - Rebuild/re-image costs
- Cost of a breach

Less Obvious Direct Cash Buckets

- De-clutter other controls
  - Other endpoint products (agent reduction)
  - Other control products
- Extending PC and server lifecycle
  - Headroom back due to performance
- Other IT operations costs
  - EOL'd systems – delayed upgrades
  - Change patching windows
  - Servers can be protected – normally cannot complete disk scan with AV
  - Reduce infrastructure costs due to less "chattiness" with cloud

Cost of Control Friction

- Controls are a “drag coefficient” on business velocity
  - Slow the user
  - Slow a business process
- Too much control friction
  - Business and users go around security and IT
    - Adds cost – IT isn’t managing IT anymore
      - Data and business silos are created
      - Loss of purchasing power
  - Adds risk
    - Risk and Security team becomes blind – can’t prevent, hard to detect
- Business adheres to the controls – generates systemic business risk
  - Lose time to market
  - Lose ability to innovate
  - Lose long-term market leadership

Example 1: No Hard Drive Leaves Intel – circa 2006

Flawed Control

40% Failure Rate

U.S. business on NBC NEWS.com

Intel to lay off 10,500 in major restructuring

Chip-maker seeks to reverse sinking profits and regain market share

Associated Press

updated 9/6/2006 10:09:39 AM ET

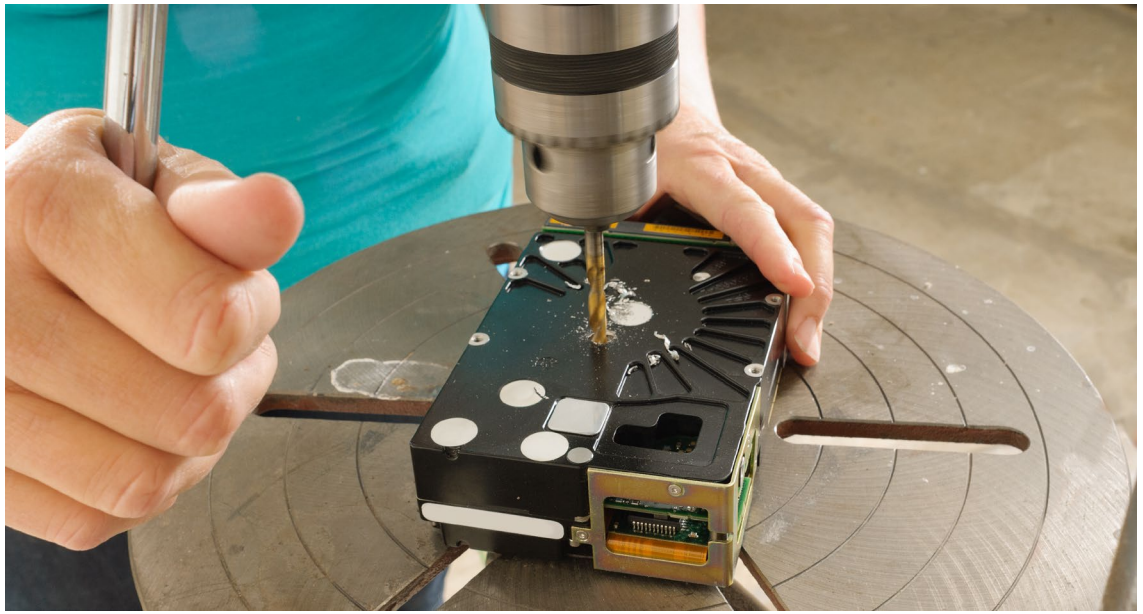
Santa Clara-based Intel said most of the job cuts this year will come from its management, marketing and information technology ranks, and will expand in 2007 to include manufacturing, design and other segments.

Flawed Control

No Money for Remediation

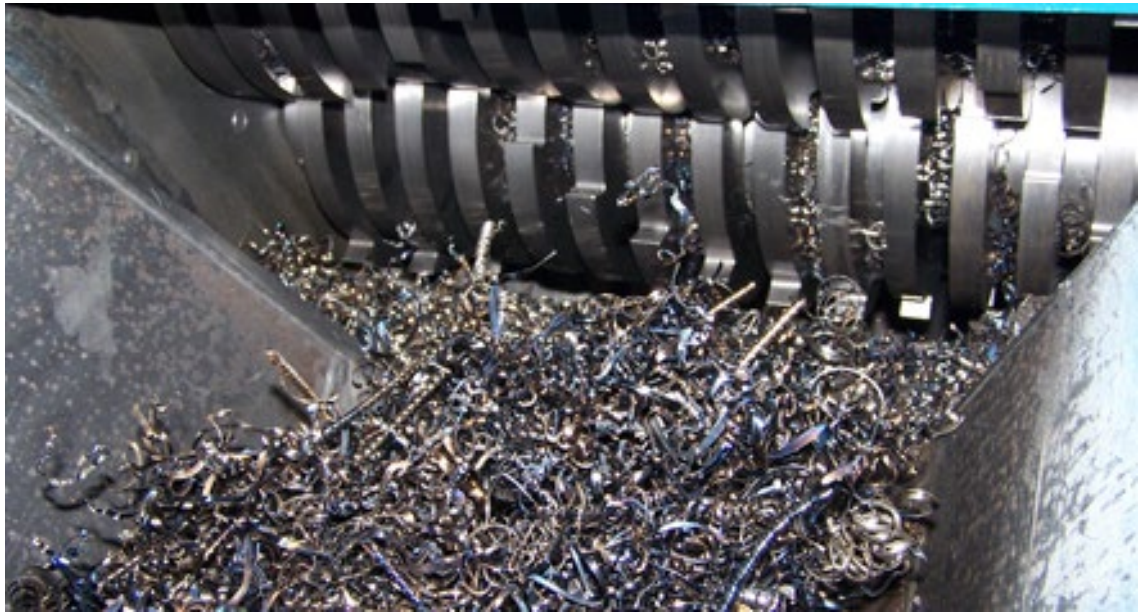
$5M in new equipment plus $2M annually for labor

Innovation Comes Through Starvation



Manual Control

Equipment $50,000
Labor $20 per hour
Over 30,000 hard drives a year



Strong Control

No $$$ Needed
Bonus – Recycling Benefit

Example 2: 14,000 ATM Machines – Windows 2003

Flawed Control

Unable To Patch

Traditional AV : 20-40% effective

the INQUIRER

Microsoft to charge $600 per server for Windows Server 2003 holdouts

The bill could run to millions

17 February 2015

Chris Merriman

@ChrisTheDJ

Flawed Control

~$8.4M for Support - “the potential to get a patch”

Traditional AV consumes ~10% of system performance

Upgrades Are Expensive and Patching Is No Panacea

"GreenDispenser" ATM Malware Allows Attackers to Steal Cash

By Eduard Kovacs on September 25, 2015

Corporate Security & Fraud Management
DIEBOLD NIXDORF
GLOBAL SECURITY ALERT

27 First 'Jackpotting' Attacks Hit U.S. ATMs

JAN 18

ATM "**jackpotting**" — a sophisticated crime in which thieves install malicious software

Insufficient Control

Upgrade ATM Equipment $140M

+ Labor to install

+ Other applications require updates

+ Cost of continued patching

Traditional AV still…

Strong Control

AI/ML pre-execution prevention tech - $300,000

Includes – device control, application control, memdef

$3M to $5M – additional network segmentation

$2M other ATM fraud mitigation

Example 3: Data Loss

OVERSIGHT
& GOVERNMENT REFORM
EST 1814

The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

"Had the company taken action to address its observable security issues prior to … cyber attack, the data breach … have been prevented."

The Anatomy Of Expense In Depth

Pandora's Box

Insufficient and … Control

Patch… | Network and Host IDS
Vulnerability Scanning Tool | Encryption
Traditional AV | DLP

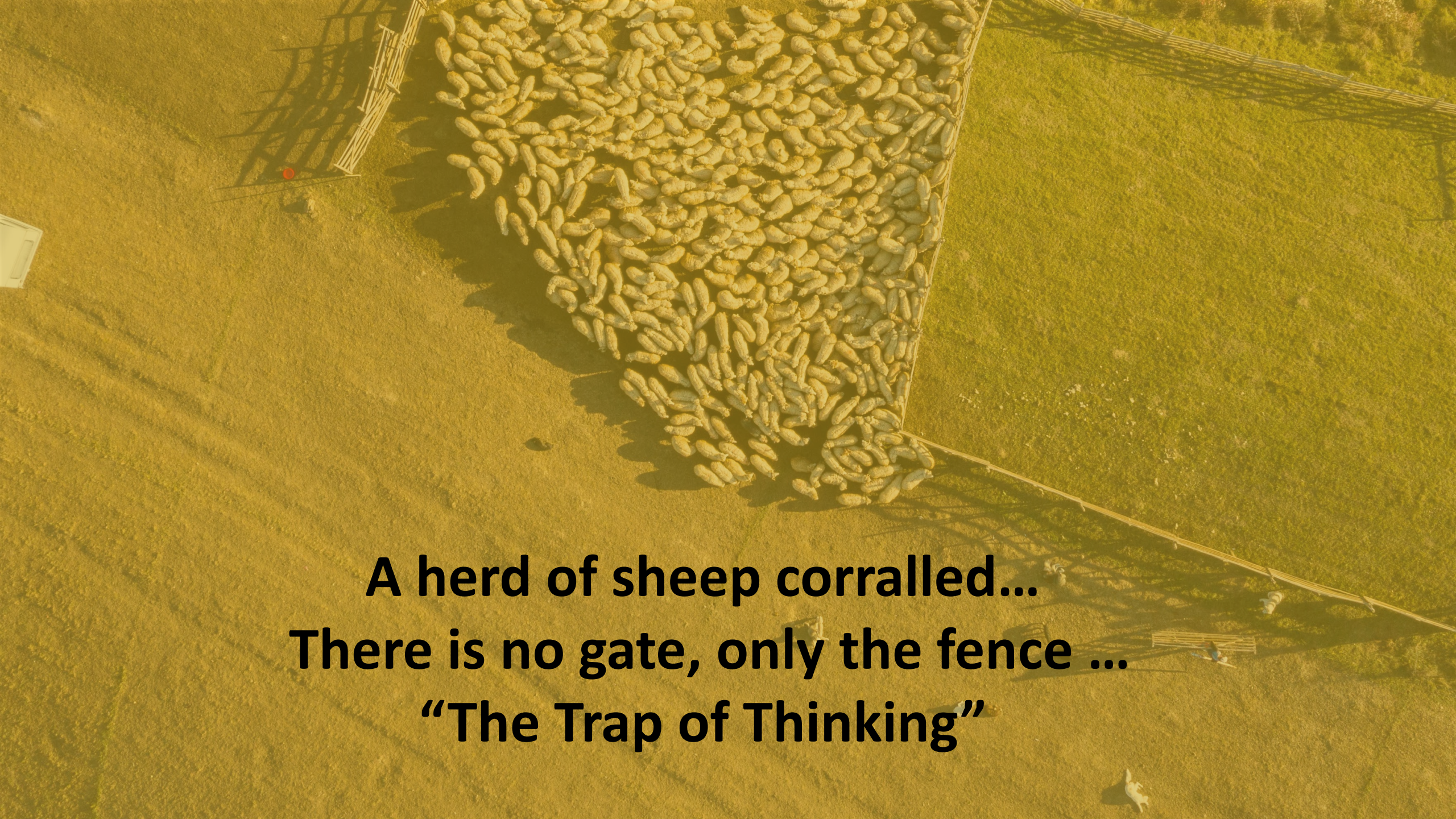
+ more tools and lots of labor

The Report contained 11 remedial rec…

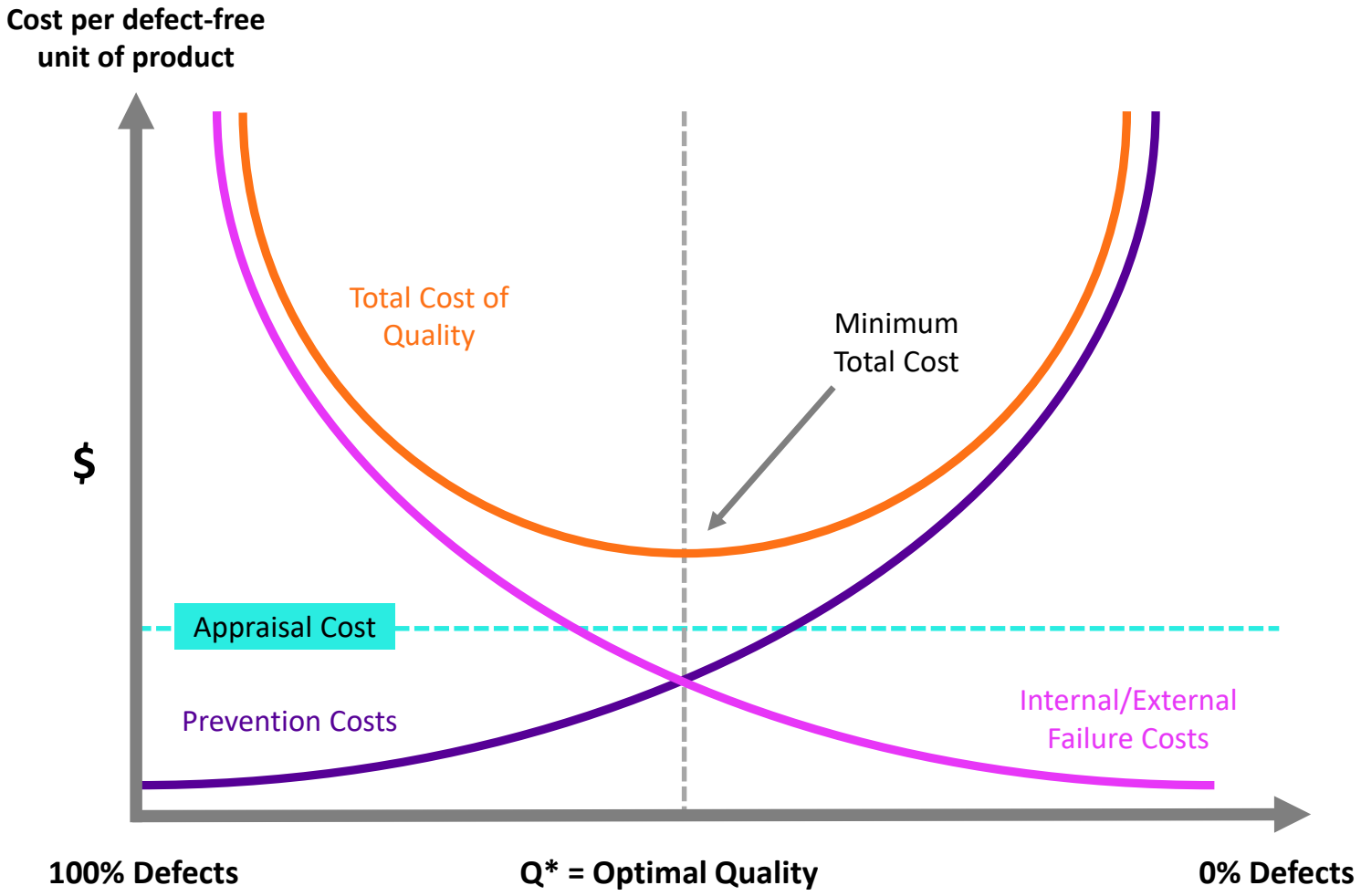
1. **Enhance vulnerability** … processes and procedure… retained in backend data… controls for accessing da… **Enhance network segme…** facing systems to backend… **web application** … attacks; 6. **Accelerate** … monitoring technologies on… **Enforce additional network** … **Accelerate de…** …ged account … solution; 9. **Enha…** for encrypted traffic by deploying additional inline network traffic decryption capabilities; 10. **Deploy additional endpoint detection** and response agent technologies; and 11. **Deploy additional email protection** and monitoring technologies.

Flawed Control

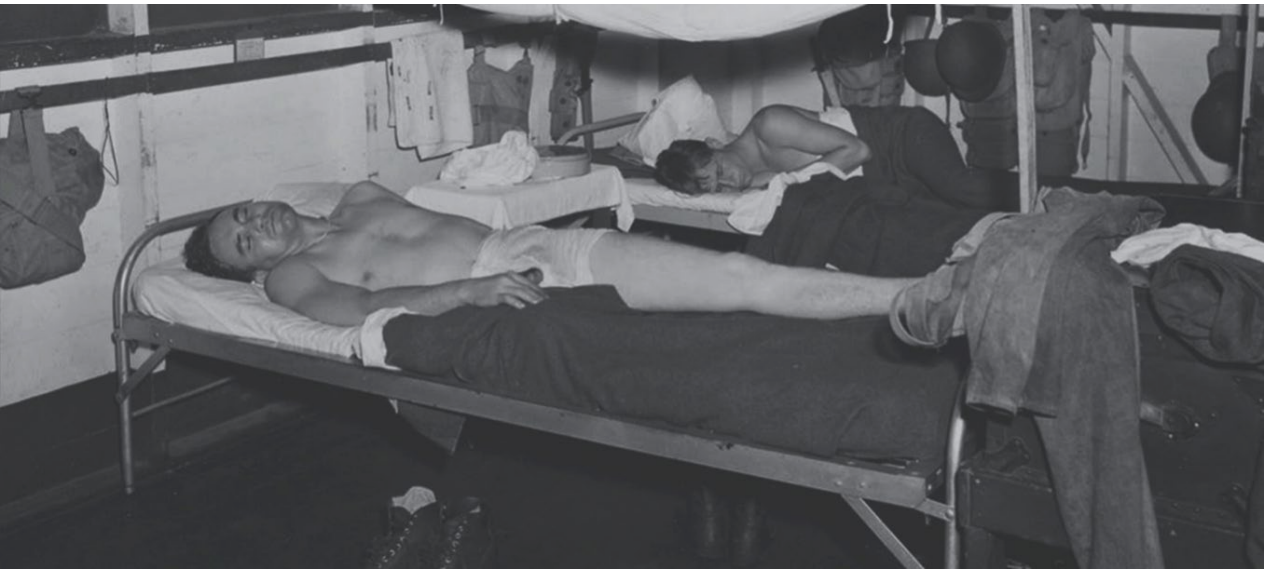
"Do More of the Same"


A herd of sheep corralled…
There is no gate, only the fence …
“The Trap of Thinking”

Total Cost of Quality, Traditional View



Prevention and Panama



How It Began

In 1879, the French started building the Panama Canal.

Torrential rains averaging 200 inches a year washed away much of the work.

A Toxic Control

The Solution? Quinine…

…but the quinine used to treat malaria left many workers deaf.

The Timeline

1903

Panama declares itself a country. U.S. gains construction rights.

Feb. 1904

U.S. Congress officially created the Panama Canal Zone.

1909

Work on canal locks begins.

1913

Panama Canal finishes.

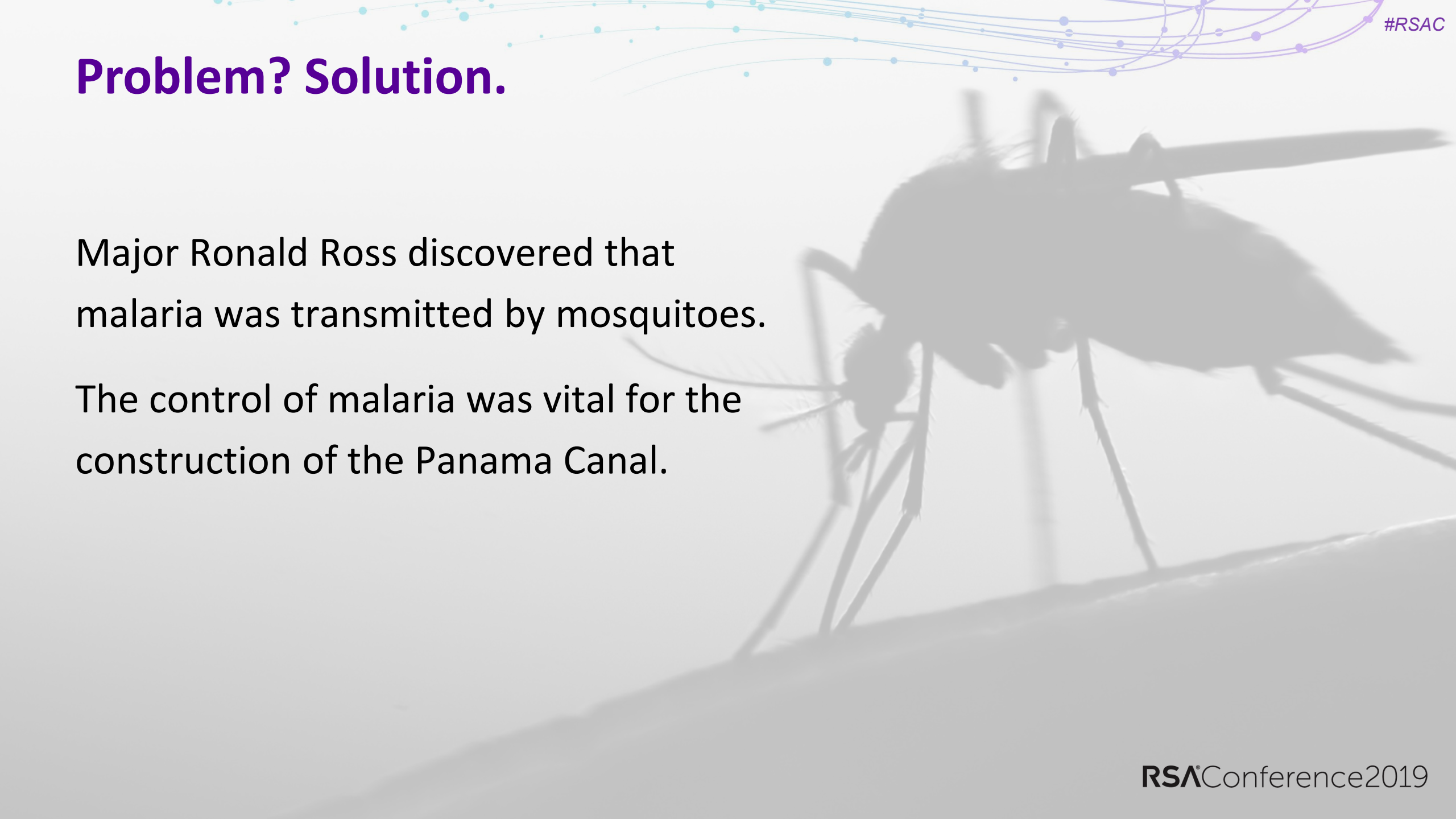
Aug. 15, 1914

Canal officially opens in August.

Problem? Solution.

Major Ronald Ross discovered that malaria was transmitted by mosquitoes.

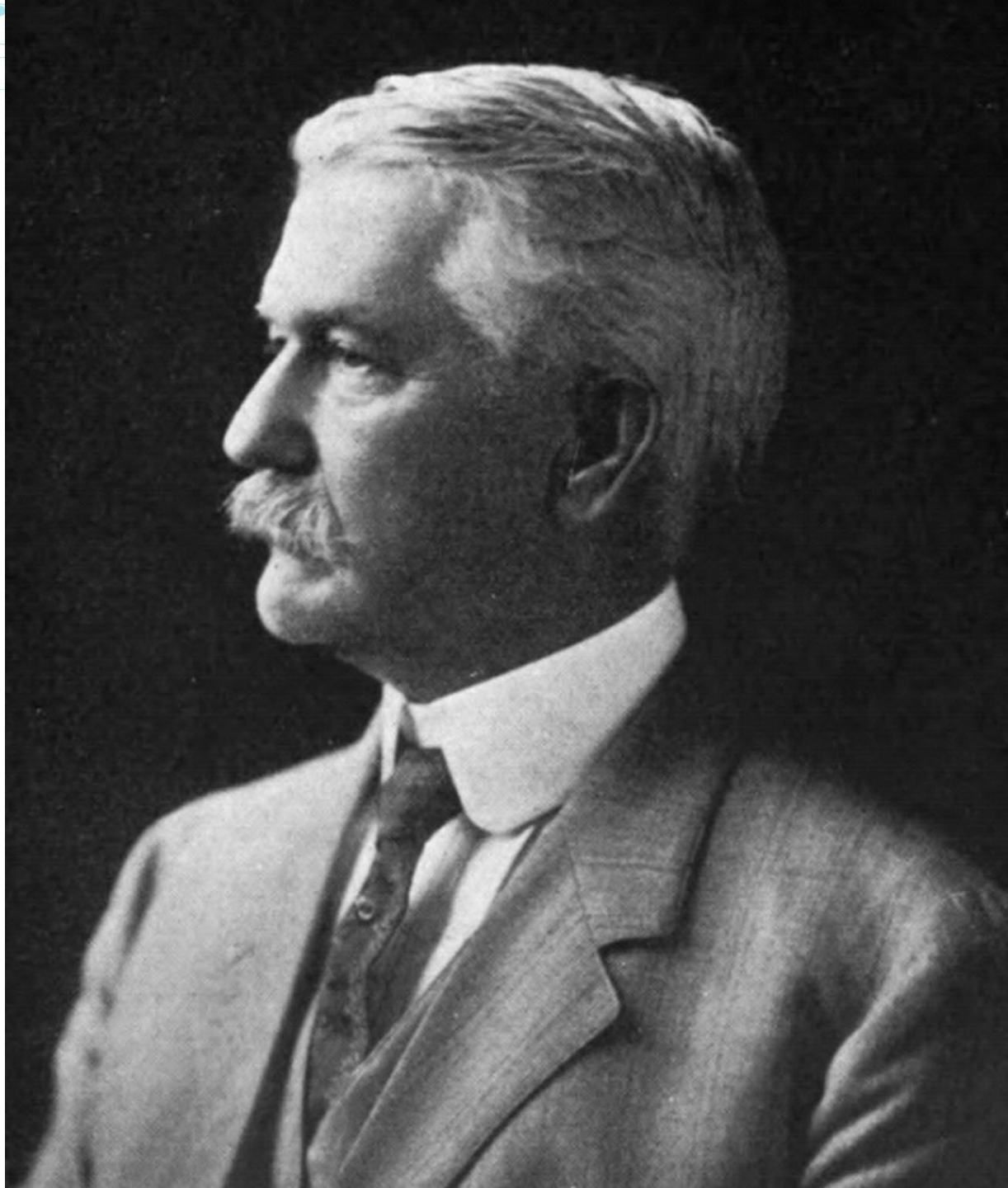
The control of malaria was vital for the construction of the Panama Canal.



A Man… His Plan… And A Canal.

Experts on sanitation.

Col. W.C. Gorgas, along with others in 1904, formed the sanitary department for the canal zone.



Malaria Control Program Results

- Eradication of yellow fever
- Death rate dropped in workers from 11.59 per 1,000 in November 1906 to 1.23 per 1,000 in December 1909
- Death rate dropped in total population from 16.21 per 1,000 in July 1906 to 2.58 per 1,000 in December 1909

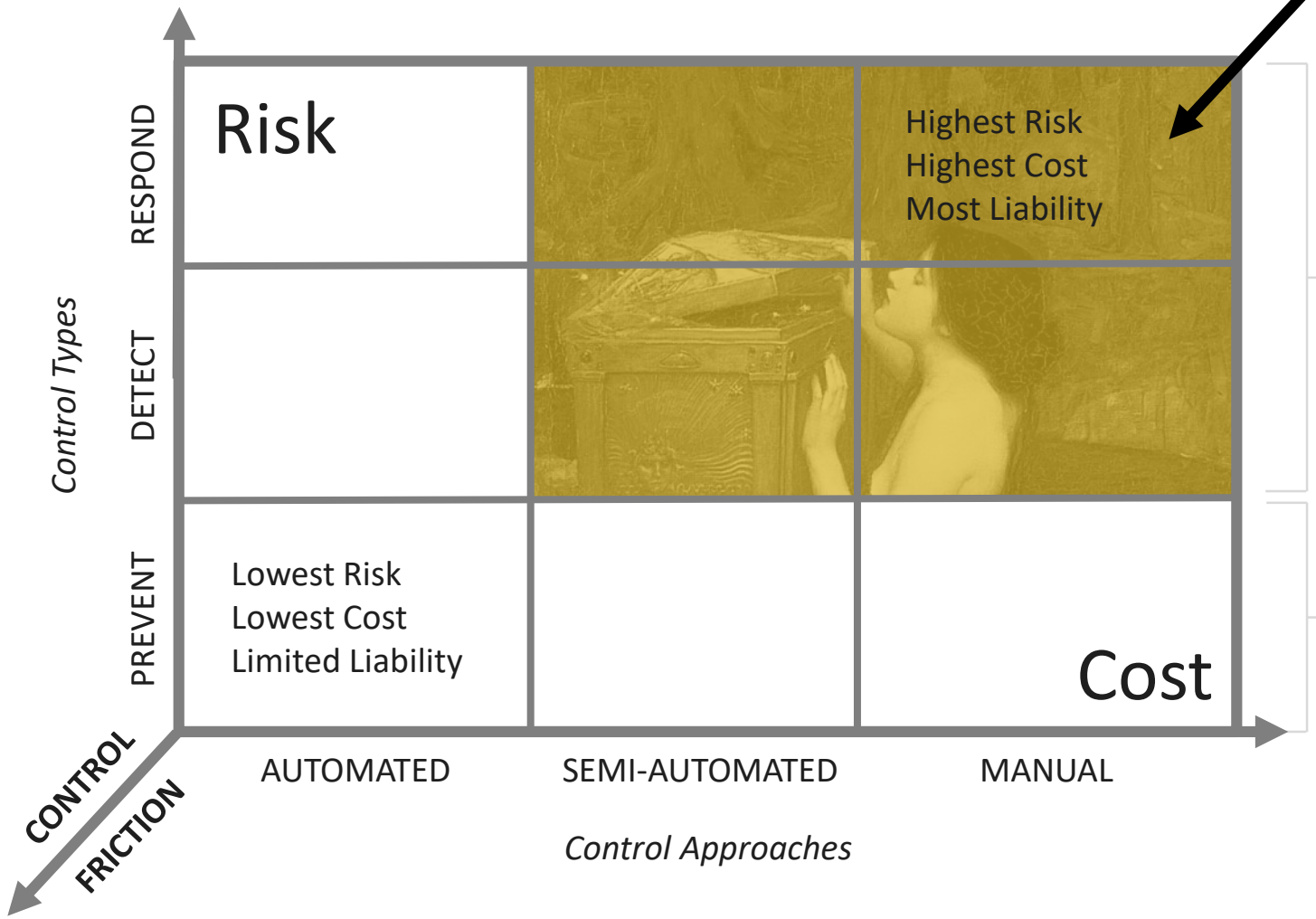
Economic Efficiency

The construction of the panama canal was made possible only after yellow fever and malaria were controlled.

Lessons for Security

Malaria wasn’t eliminated, but the root causes were identified, the **source of problems were prevented**, and construction was completed, **leading to dramatic worldwide social and economic benefit.**

9 Box of Controls



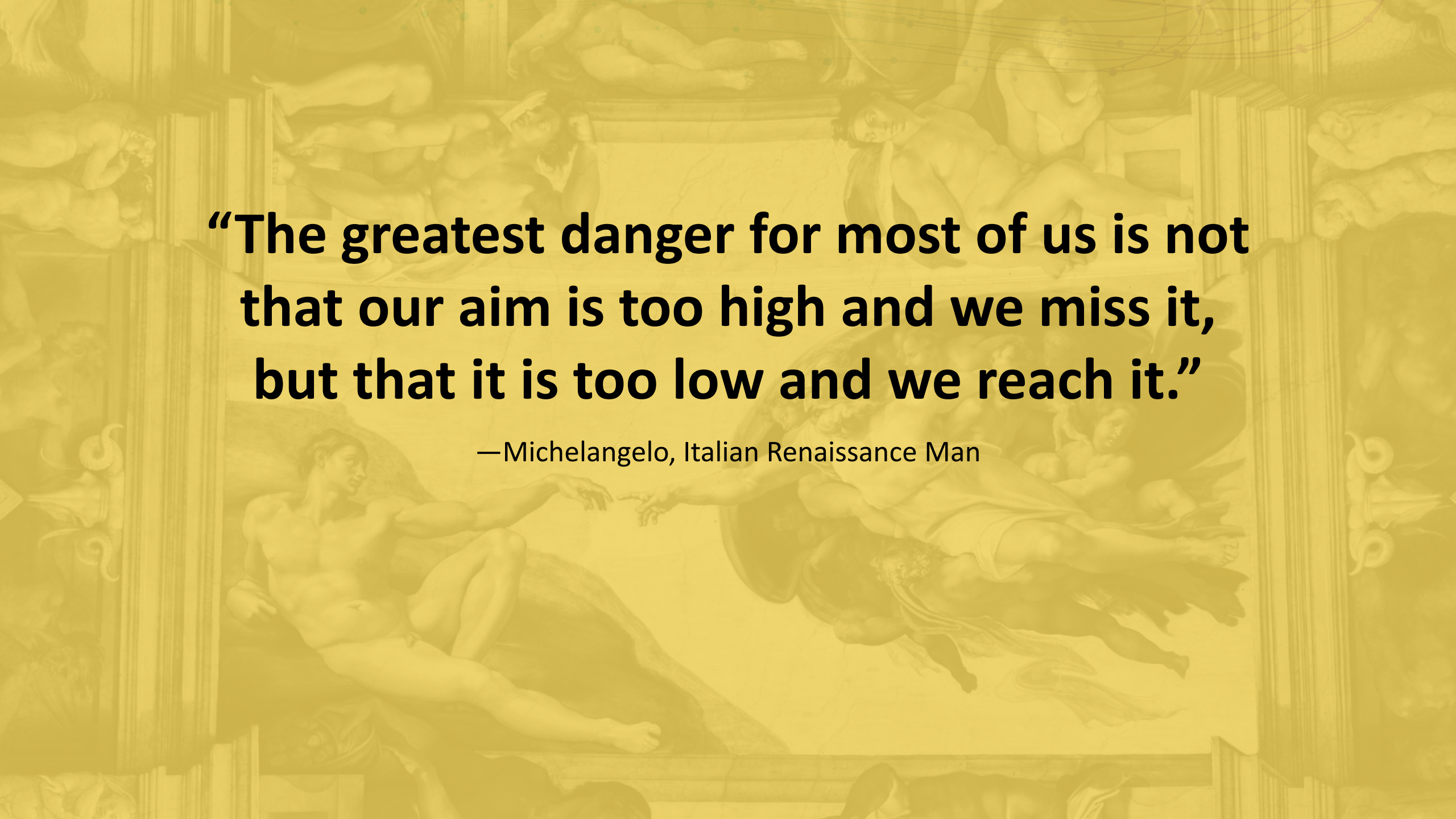
Pandora's Box

Where most of the industry is focused

Focus is on minimizing damage – only variables are time to detect and time to contain

Focus is on minimizing vulnerability and potential for harm

Source: Managing Risk and Information Security 2nd edition Malcolm Harkins



“The greatest danger for most of us is not that our aim is too high and we miss it, but that it is too low and we reach it.”

—Michelangelo, Italian Renaissance Man

THE MOMENT …

The Anatomy Of Expense In Depth

Pandora’s Box

1%

The Anatomy Of Expense In Depth

Pandora's Box

““Accept it…they are going

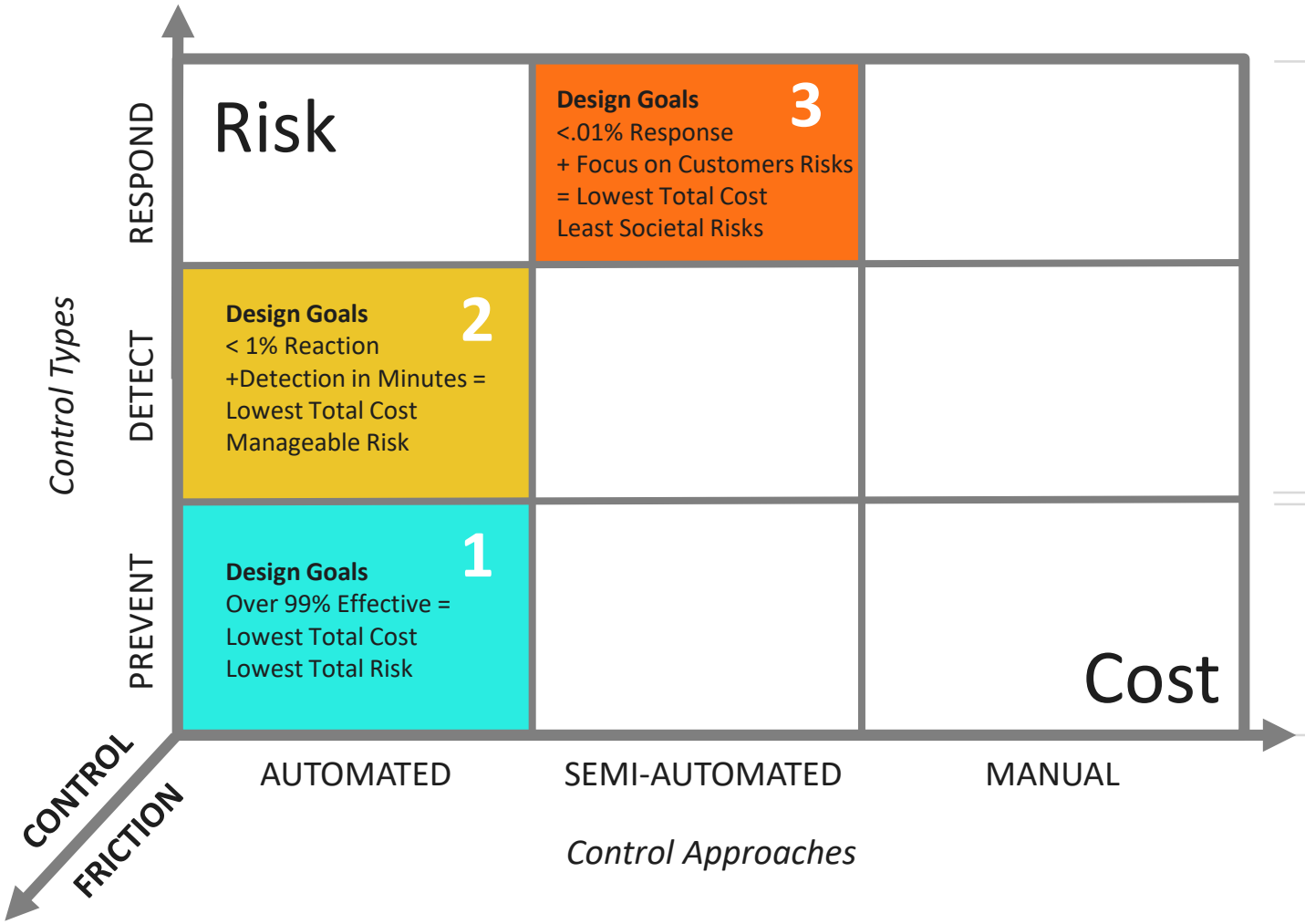
The Anatomy Of Expense In Depth

Pandora’s Box

“The problems of the world cannot be solved by skeptics or cynics, whose horizons are limited by the obvious realities. We need men who can dream of things that never were and ask why not … the humblest nation of all the world, when clad in the armor of a righteous cause, is stronger than all the hosts of error”

—John F. Kennedy,
Address before the Irish Parliament, June 28, 1963

9 Box of Controls

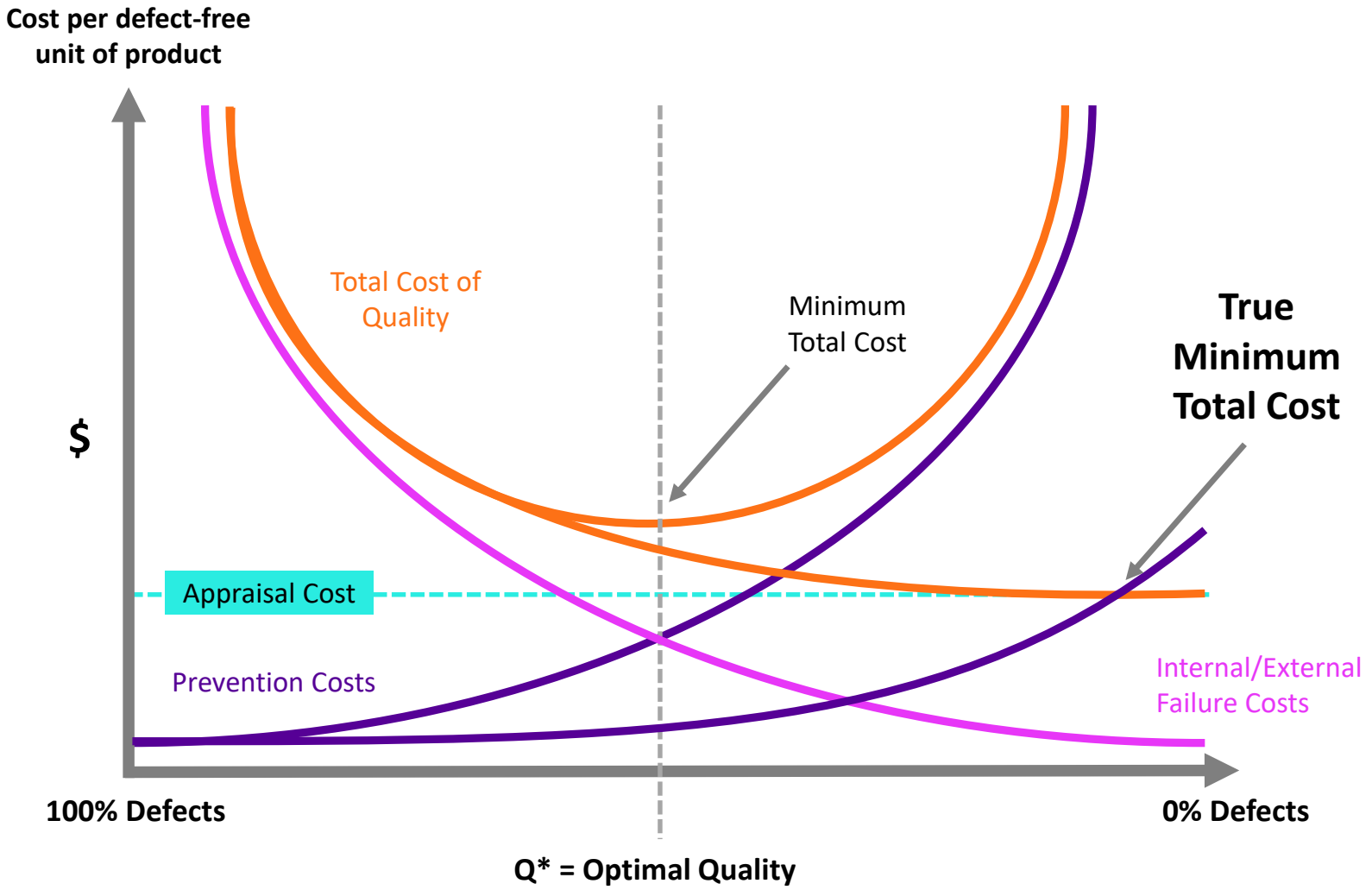


Focus is on minimizing damage – only variables are time to detect and time to contain

Focus is on minimizing vulnerability and potential for harm

Source: Managing Risk and Information Security 2nd edition Malcolm Harkins

Total Cost of Quality, Possibility Thinking – 9 Box of Controls



Applying the Lessons

BETTER.

1. Treat information security as an economic inefficiency
2. Understand total costs
3. Understand strong control design

Applying the Lessons

BETTER.

1. We need to create a demonstrable and sustainable bend in the curve of risk
2. We need to lower / flatten the total cost of controls
3. We need to reduce the control friction on our users and on our businesses

Applying the Lessons

1. Hold the security industry accountable for its failures
2. Focus on societal risk
3. Stop accepting compromise

“…where our interests are clear and our values are at stake, and we can make a difference, we must act and we must lead.”

—Madeline Albright, “Doability Doctrine”
Statement before SFRC January 8, 1997, Stockholm Sweden

Better Only Happens If

We break the Greek myths

and Elpis leaves Pandora's

Myths Busted