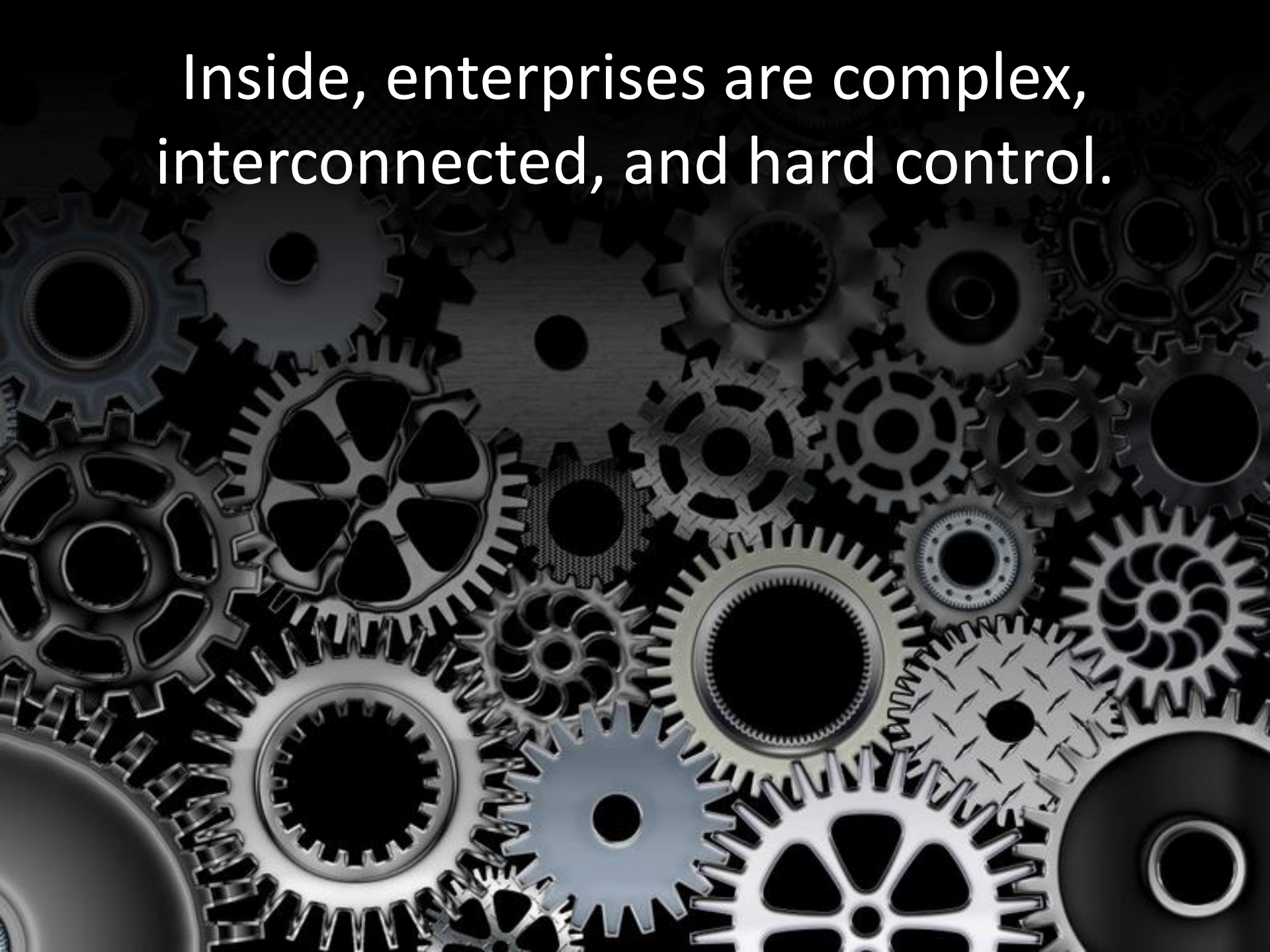
Data Breaches and the Insider Threat: What to Do?

Lenny Zeltser

www.zeltser.com

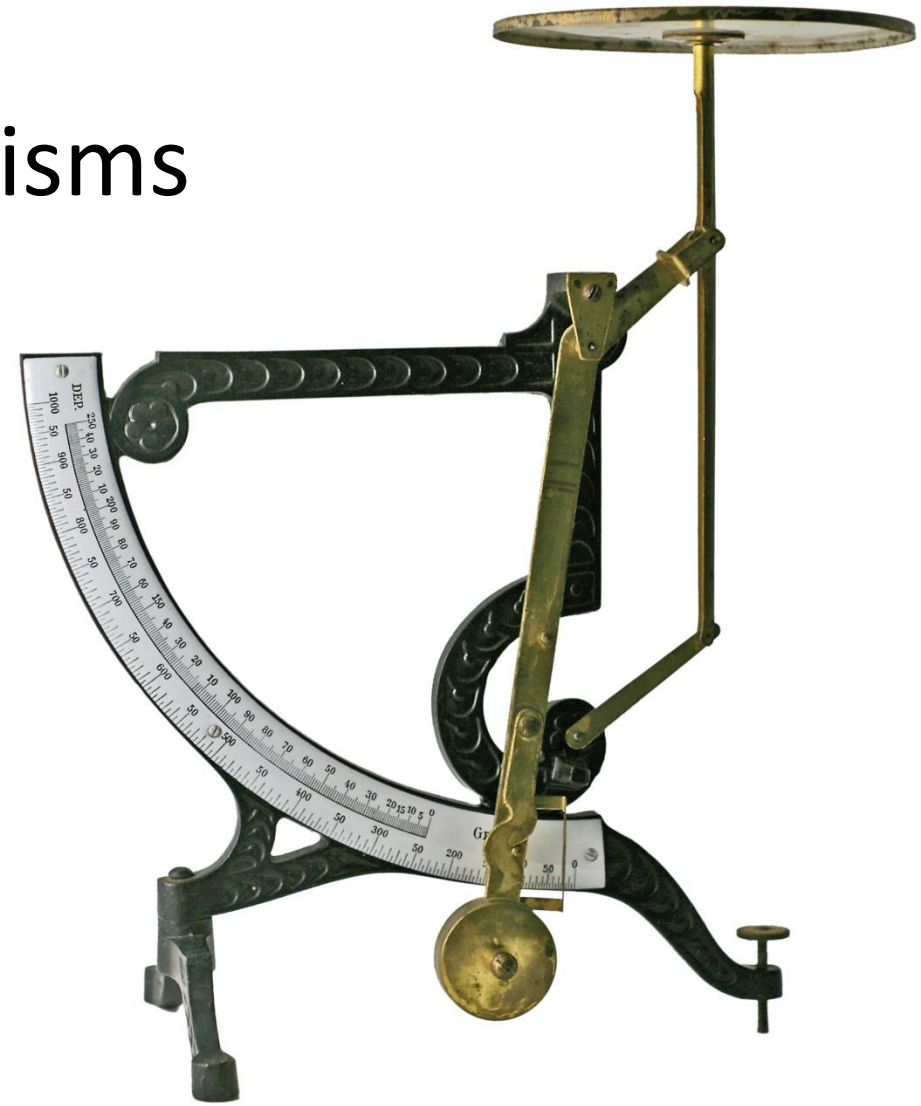

Layered perimeter defenses tend to
focus on external threats.

Inside, enterprises are complex, interconnected, and hard control.



Many of today's breaches are the result of an insider's actions.

Balancing policy, preventative, and monitoring mechanisms helps address the insider threat.



Let's survey a few recent breaches and consider mitigation strategies.

Inadvertent Insider Breaches

UK Ministry of Defence laptop stolen with data of 600,000 would-be recruits

Social Security numbers on mailing labels to Wisconsin health care recipients

ABN Amro spreadsheet with customer records leaked via file sharing network

Employee e-mailed out personnel details of Cameron County workers

University of Pittsburgh Medical Center left patient data on a website

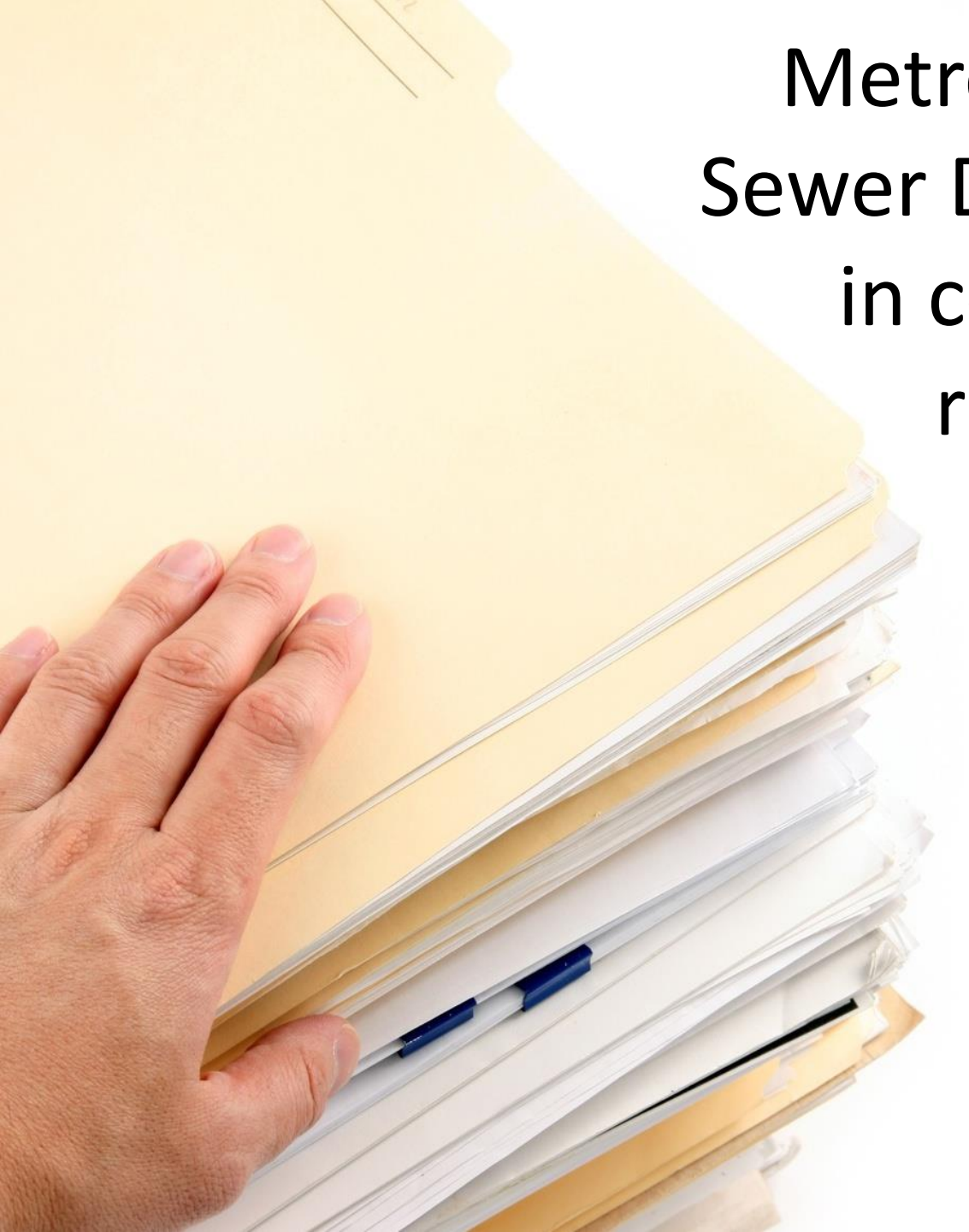
SAIC transmitted military family records without encryption over the Internet

Weak controls around data dissemination

Unclear processes for “secure” data handling

Slow detection capabilities

Malicious Insider Breaches



Metropolitan St. Louis Sewer District employee in copied records for retaliation against employer

Pfizer employee copied co-workers' records

Electronic Data Systems ex-employee sold identities of Medicaid recipients

Fidelity National Information Services worker stole customers' financial records

Overly-permissive data access practices

Weak access monitoring capabilities

Weak leakage detection capabilities


Data breaches seem to be increasing in frequency and severity.

The breaches are often self-inflicted by insiders—maliciously or accidentally.

People are good at bypassing controls to get work done or to earn a profit.

Clarify which are the prohibited activities and…

… document processes for sharing information in an approved manner.

Provide data sharing mechanisms and training to employees.

Enforce the data-sharing policies.

Monitor data traversal and access to deter, detect, and investigate breaches.

Lenny Zeltser

www.zeltser.com
lenny.zeltser@savvis.net