



ISACA[®]

Trust in, and value from, information systems



ISACA Ireland Conference 2017

October 20th

www.isaca.ie

A New Paradigm – Asset-oriented Risk Management

Joseph Mayo

J. W. Mayo Consulting, LLC



A Call to Action

Federal Bureau of Investigation (FBI) estimated organized crime generates \$1 trillion in cyber crime profits annually

\$1 trillion profit can sustain an annual R&D budget of \$478 billion

Top-24 companies in the world spent an estimated \$110 billion on all R&D activities

Criminals spend more than 4 times what legitimate organizations do on R&D



A Call to Action

IT budgets range between 4% - 6% of total revenue

2017 projections indicate some IT budgets will be as much as 8% of revenue

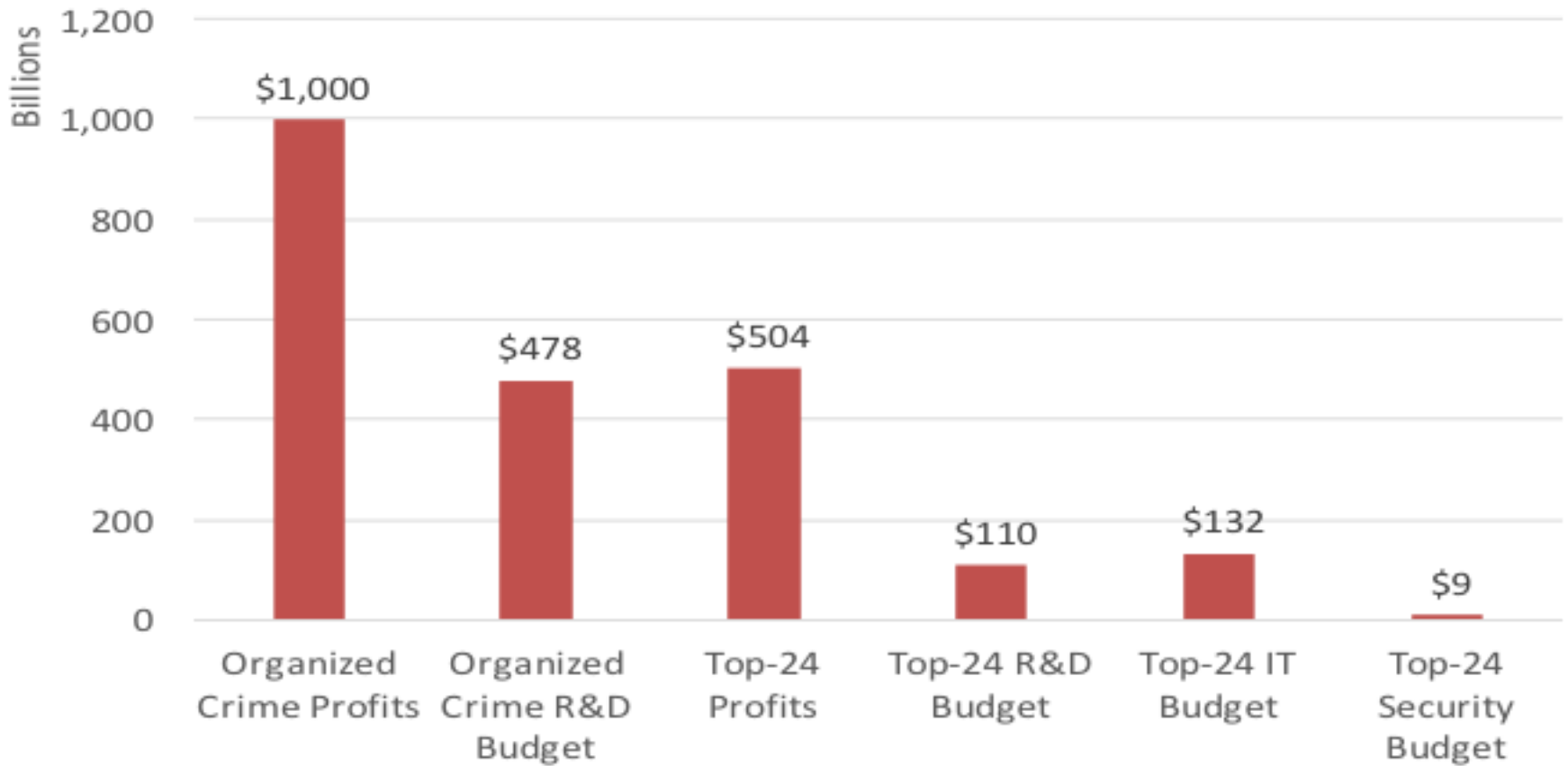
IT security budgets ranges between 1% - 13% of the IT budget

Assume the Top-24 companies allocate 6% of their revenue to their IT budget and 7% of their IT budget to security

The Top-24 are spending \$9 billion to combat a threat that is spending more than 50 times that amount to find new ways to exploit security weaknesses



Security Budgets Versus Threat Budgets





ISACA Ireland Conference 2017
October 20th
www.isaca.ie

Case Study – Sigma Pharmaceuticals



Sigma Pharmaceuticals

Tightly coupled ERM and management accounting information system (MAIS)

Comprehensive framework to identify, assess and manage risk across the enterprise

Established a Risk & Audit Committee (RAC)

Regular internal and external audits

Monthly reporting to the Board



Sigma Pharmaceuticals

Supreme confidence ERM and MAIS would provide early warning for emerging risk event

RAC was heavily compliance focused on near-term risk events

February 2010 Sigma shares plummeted 58% in one day and ultimately collapsed nearly 80%

Sigma shares were suspended from trading and Sigma was nearly bankrupt overnight

The cause was a low probability, high impact risk that had been reported for quite some time



Sigma Pharmaceuticals

What went wrong?

- **Multiple risk events simultaneously**
- **Risk events occurred out of sequence**
- **Risk events were low probability**
- **Tightly coupled ERM and MAIS did not detect these events**
- **Blind faith in ERM process and Compliance-based approach set the stage for a devastating domino effect**



What We Learned From Sigma

Tight coupling can lead to a domino affect impossible to stop

Non-linear complexity of risk can result in unpredictable behavior and results

Pure compliance-based auditing is insufficient



What Do We Do Now?

Focus on asset protection

- **Process compliance is necessary but is secondary**
 - **Assets include**
 - **People (employees, suppliers, customers, contractors)**
 - **Intellectual property (patents, processes, methods, etc.)**
 - **Property (buildings, fleets, IT, real estate, etc.)**
 - **Data**
 - **Reputation**
- **Migrate from compliance-based auditing to heuristic auditing**
- **Challenge the status quo**
 - **Are we doing enough?**
 - **Are we doing the RIGHT things?**
 - **Just because we have always done it this way, is this the right thing to do?"**
 - **Are we running on trust (and being lucky) or are we really protected**



ISACA Ireland Conference 2017
October 20th
www.isaca.ie

Heuristic Auditing



Heuristic Auditing

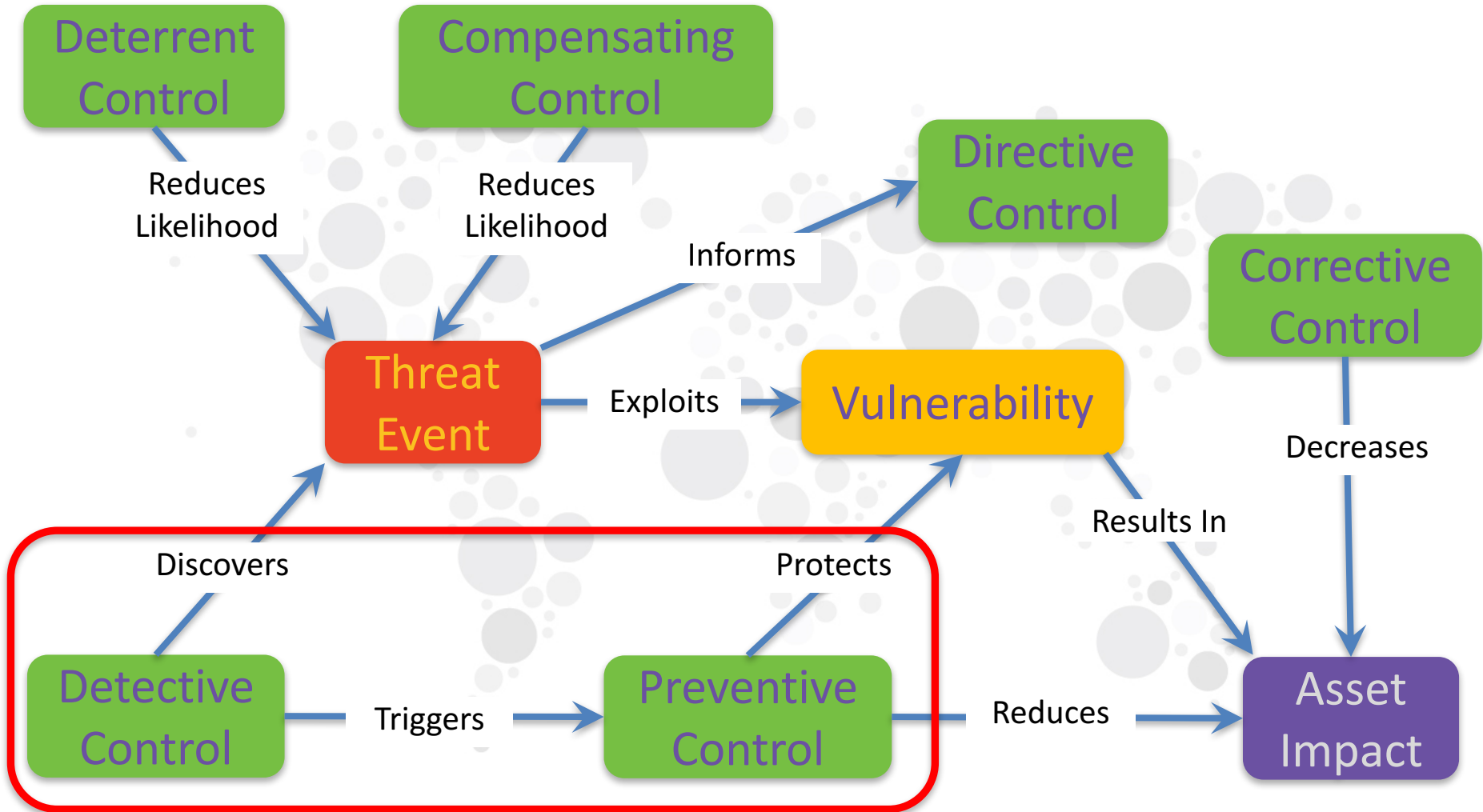
Heuristic (adjective | heu·ris·tic | \hyu-'ri-stik\)

1. involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-an-error methods
2. of or relating to exploratory problem-solving techniques that utilize self-educating techniques to improve performance

Primary focus is asset protection

Follow your nose approach

Consider incidents and near-misses as learning opportunities





Conclusion

Organizations can not compete financially with criminal enterprises

We must revolutionize current risk management practices

Risk management must evolve from a defensive strategy to an offensive strategy

Sun Tzu - Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive.

- A defensive strategy avoids losing
- An offensive strategy allows winning

Increase use of detective controls and KRIs to provide early warning of problems

Detective controls, KRIs, and heuristic auditing will protect more assets and avoid a repeat of Sigma Pharmaceuticals



Thank You!

Joseph W. Mayo

joseph.mayo@jwmc-llc.com

@TaoOfRisk

