Strategic Leadership for Managing Evolving Cybersecurity Risks

NSF Cybersecurity Summit 2014

August 28th 2014, Arlington Virginia

Matthew Rosenquist
Cybersecurity Strategist, Intel Corp

Opportunity and Challenges

Working together to address

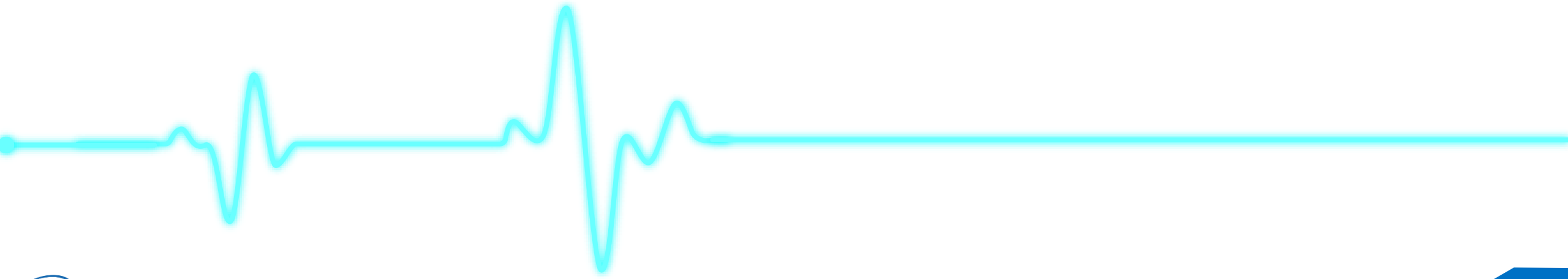
- Burning challenges of today
- Opportunities for a better tomorrow
- Many roles and uncertainty
- Embracing the best practices across the industry
- What does success look like?

Technology connects and enriches the lives of every person on earth

Security is critical to protect computing technology from threats which undermine the health of the industry

"...If security breaks down, technology breaks down"

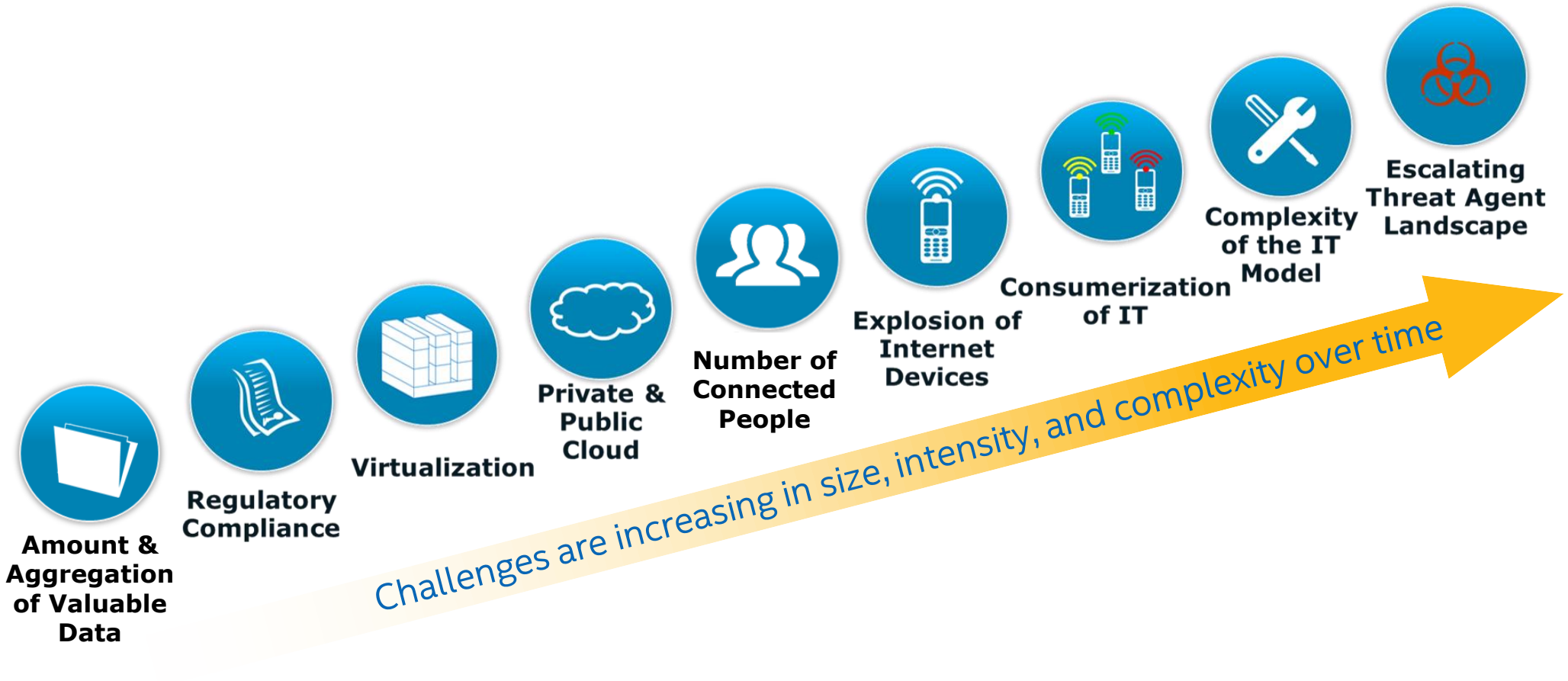
Brian Krebs
Noted Cybersecurity Reporter



We manage security through either leadership or crisis

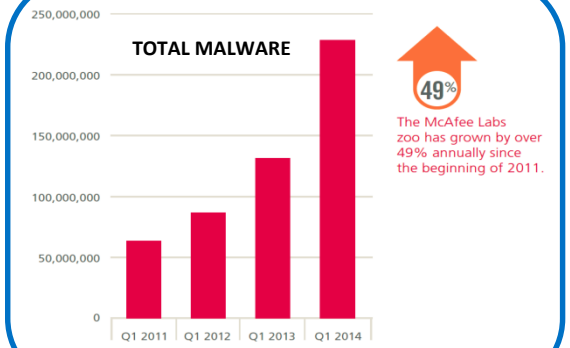
In the absence of leadership, we are left with crisis

Changing Landscape Drives Security



Security issues undermine the continued growth, innovation, and adoption of technology

Leading Metrics & Trends



Source: McAfee Threat Report Q1 2014

~300k New Malware/day
220m+ Total

~50%

Increase of 'signed' malware

Source: McAfee Threat Report Q3 2013

25m+ Total
'signed' Samples

$400b

Annual cost of global cybercrime

Source: McAfee Cost of Cybercrime report 2014

~20%-30% of overall technology spending[1]

~32%

Worldwide computers infected in 2012

Source: Panda Labs

Global Infection Rates

50%

Online adults victims of cybercrime or negative situations

Source: Symantec 2013 Norton Report

1M+ Adults Victims each day (12 per second)

93%

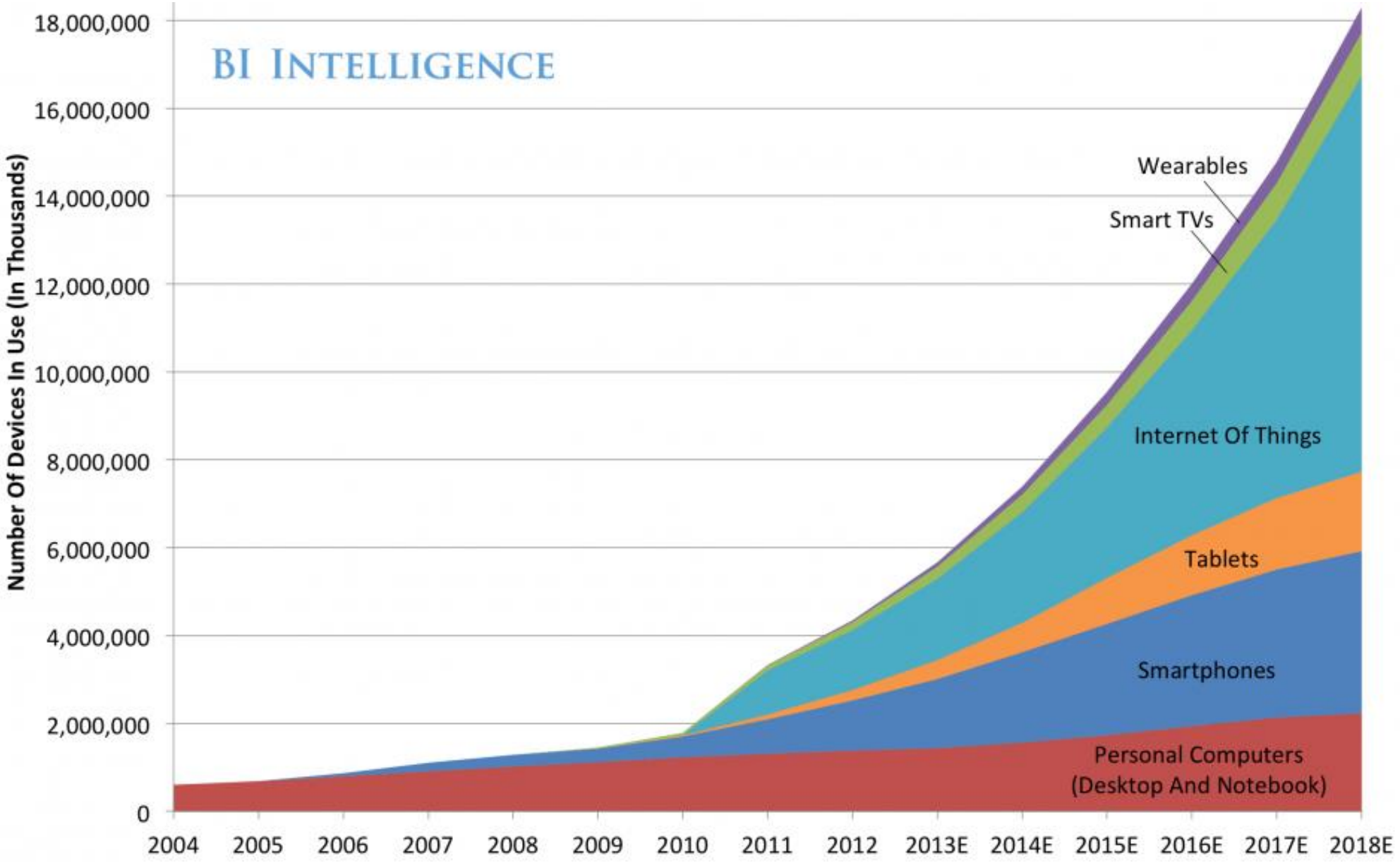
Organizations suffering a data breach in 2013

Source: UK Government BIS Survey

40% Increase in Data Breaches

intel Security

Global Internet Device Installed Base Forecast



Source: Gartner, IDC Strategy Analytics, Machina Research, company filings, BII estimates

~$3 Trillion

Aggregate economic impact of cybersecurity on technology trends, through 2020[1]

[1]Risk and Responsibility in a Hyperconnected World - 2014 World Economic Forum, http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises

Leadership is key in organizing resources to achieve and maintain an optimal level of security value

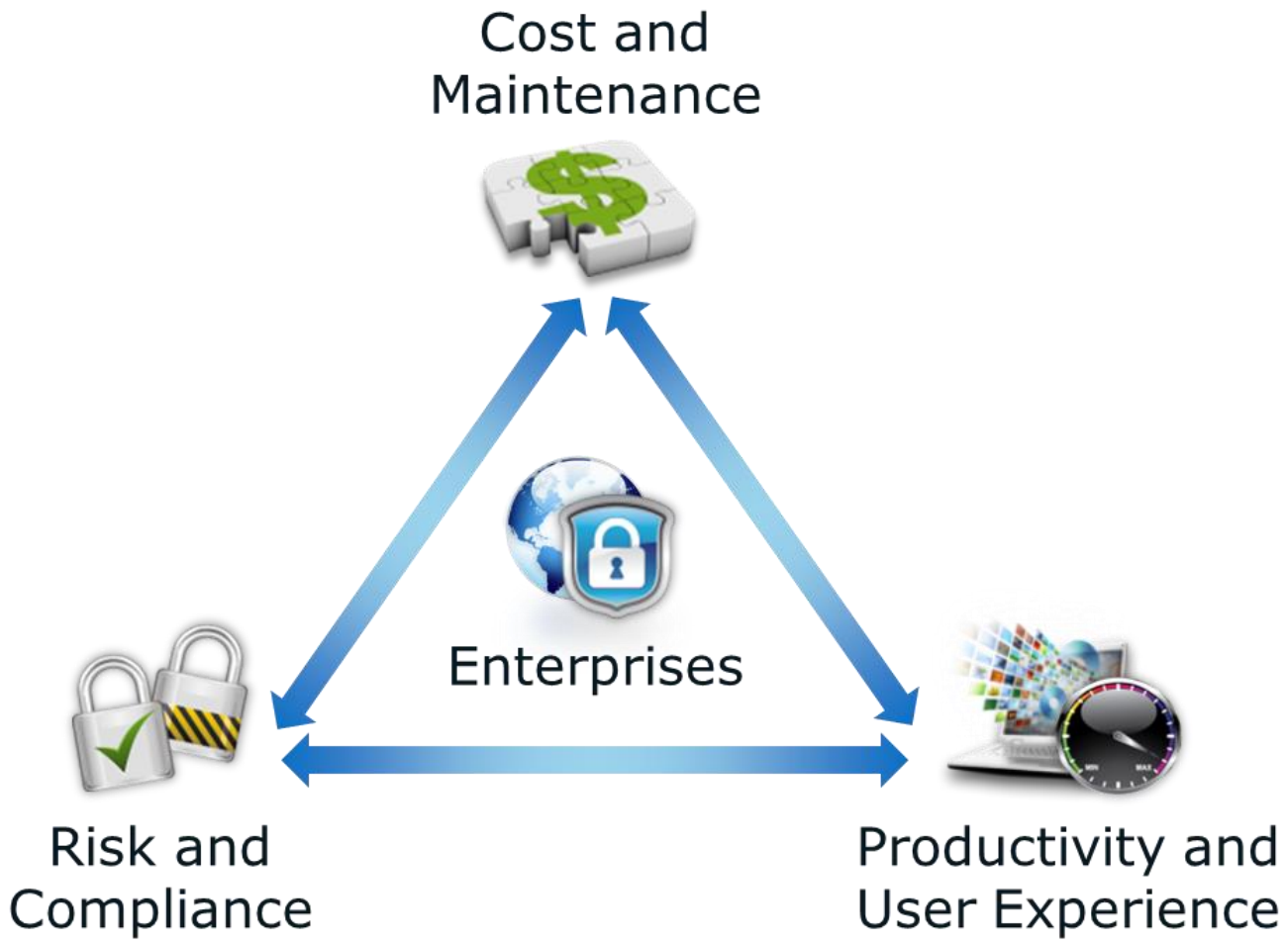
Resource Constraints and Decisions

"Infinite Resources
=
Infinite Possibilities"

Smart Decisions are Key

Balancing Security Value Aspects

Optimal security is the **right balance** of cost, user experience, and risk tradeoffs



Obstacles

versus

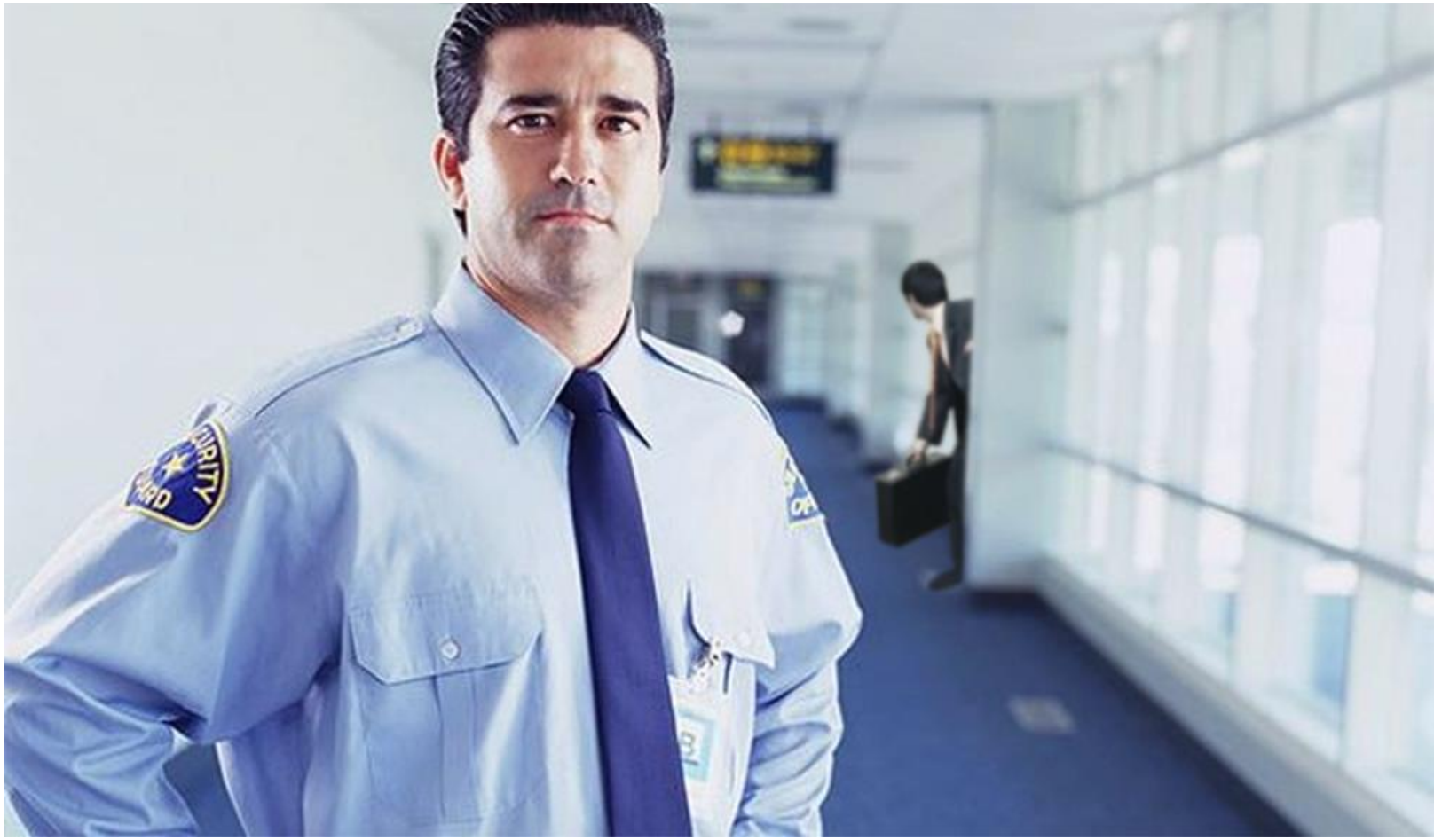
Opposition

Technical & Behavioral

Security is comprised of both **Technology** and **People**

Intertwined and inseparable

Threat agents include **Insiders** & **Outsiders**



Threats

Rise in sophistication, numbers, and resources

Users

Increasing numbers, use cases, and expectations

Threats

Trusted Users

Security Appliances

Web, Email, Voice

Enterprise Apps

Hosted Services

Storage – Local & Portable

Virtual Environments

Cloud

Internet

DMZ-Firewall

Servers

Network

PC & Workstation

Phone & Tablet

Anti-Malware Firewall/HIPS

Sensitive Data

Data

Users

APP

IT Models

Rapid growth, changing architecture, new services

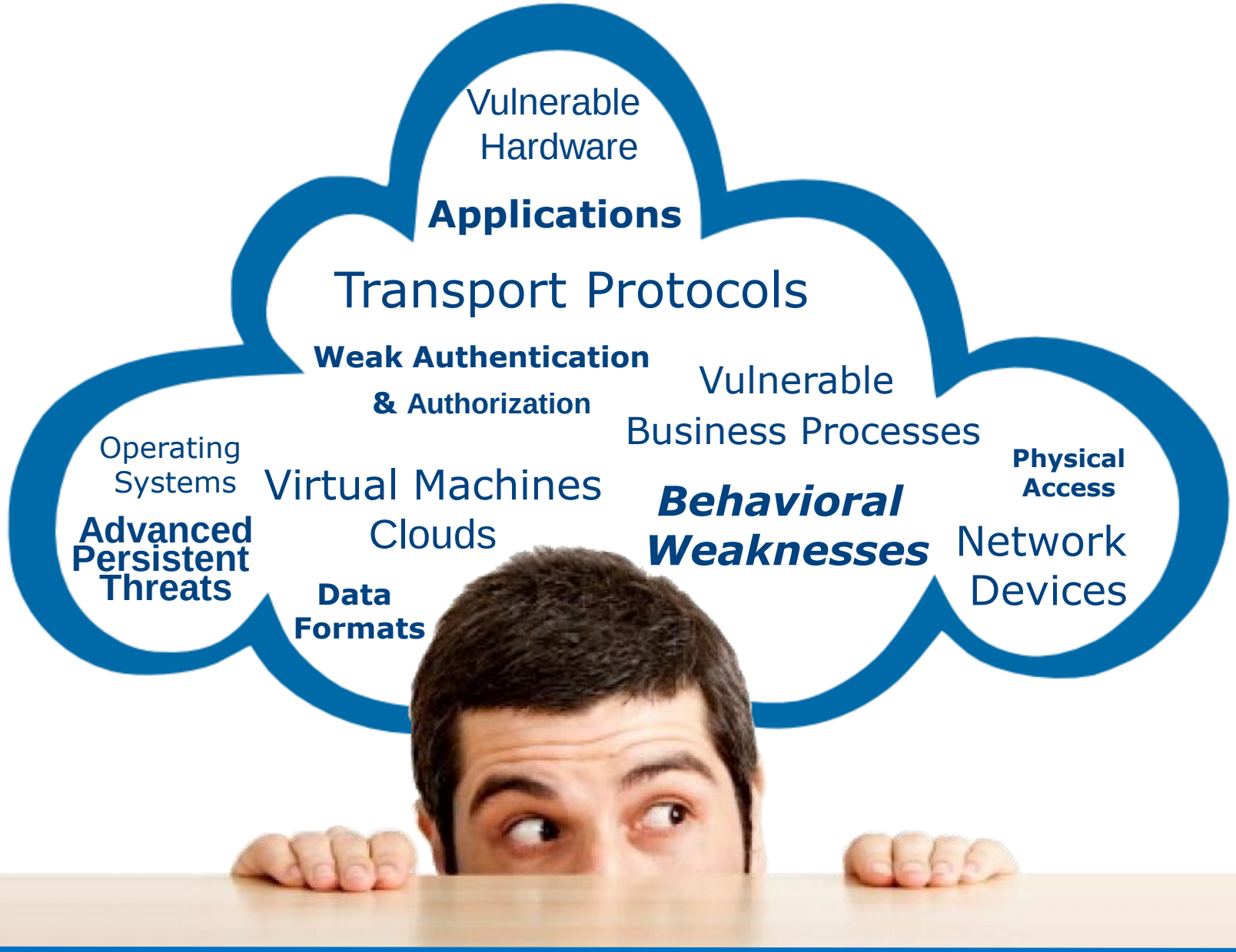
Infrastructure & Business Processes

Sensitive Data

Massive increase in data and value

An effective strategy enables operational flexibility, while driving cost efficiency, and risk manageability

Reasonable and Rational Vulnerability Management



Process: **Defense-in-Depth** Continual Security

PREDICT

Predict the most likely attacks, targets, & methods

Proactive measures to identify attackers, their objectives and methods prior to materialization of viable attacks.

PREVENT

Prevent or deter attacks so no loss is experienced

Secure the computing environment with current tools, patches, updates, and best-known methods in a timely manner. Educating and reinforcing good user behaviors.

Cyber Security Strategy

RESPOND

Rapidly address incidents to minimize loss & return to normal

Efficient management of efforts to contain, repair and recover as needed, returning the environment to normal operations.

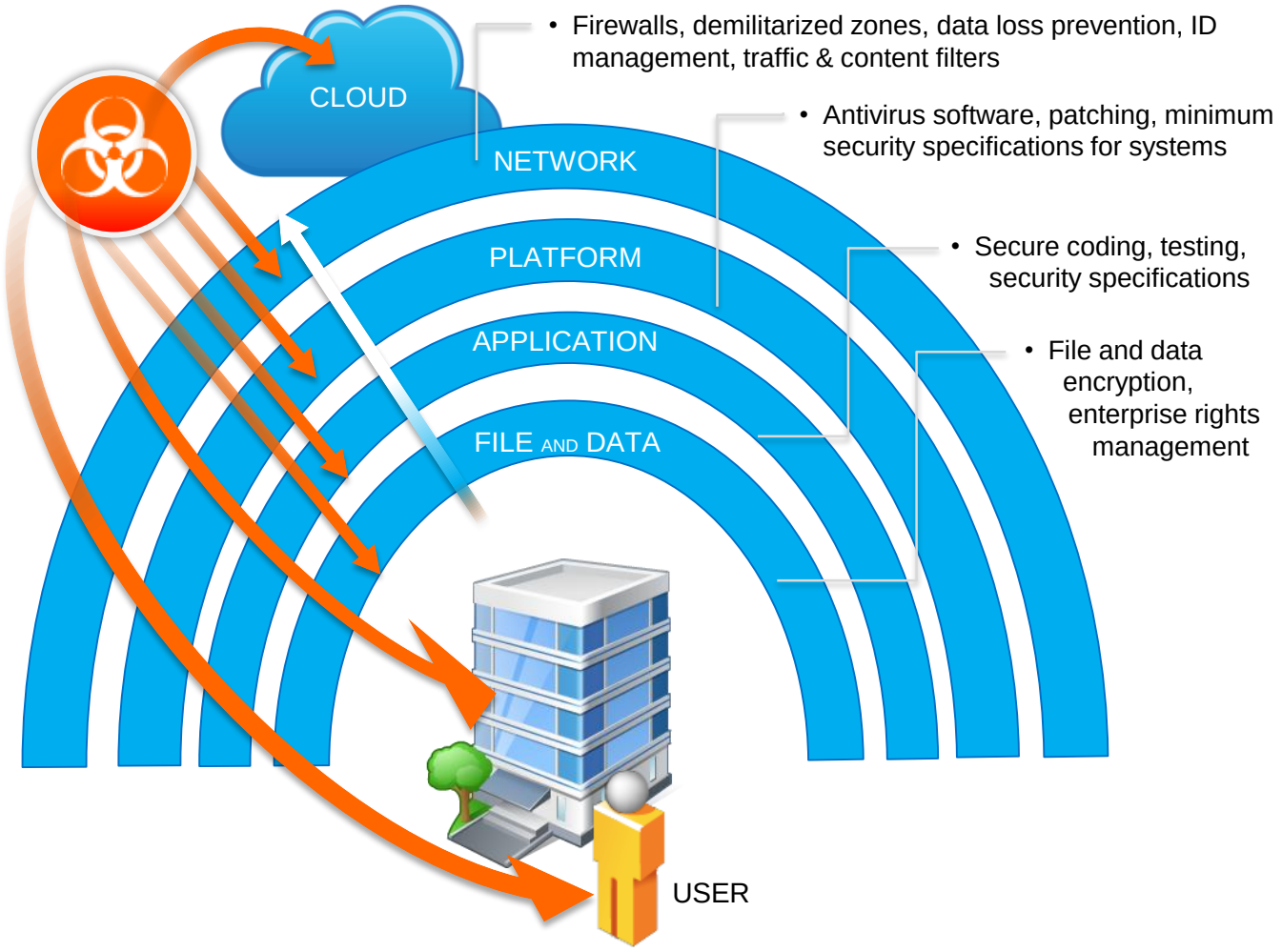
DETECT

Identify attacks not prevented to allow for rapid, thorough response

Monitor key areas and activities for attacks which evade prevention. Identifies issues, breaches, and attacks.

Layered: Security Technology Integration

Security must persist at multiple layers to insure consistency and comprehensiveness

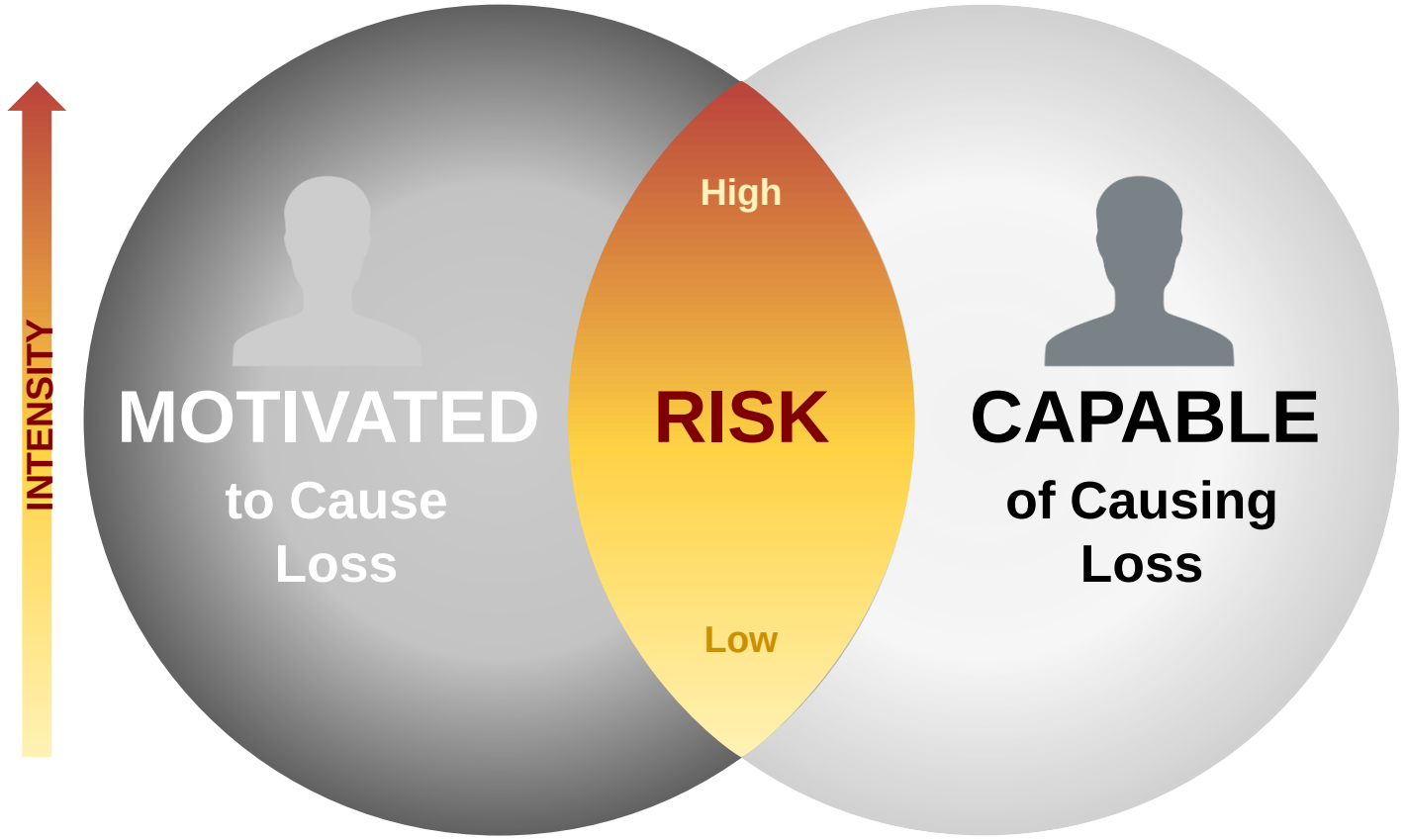


Know your enemy and know yourself and you can fight a thousand battles without disaster. – *Sun Tsu*

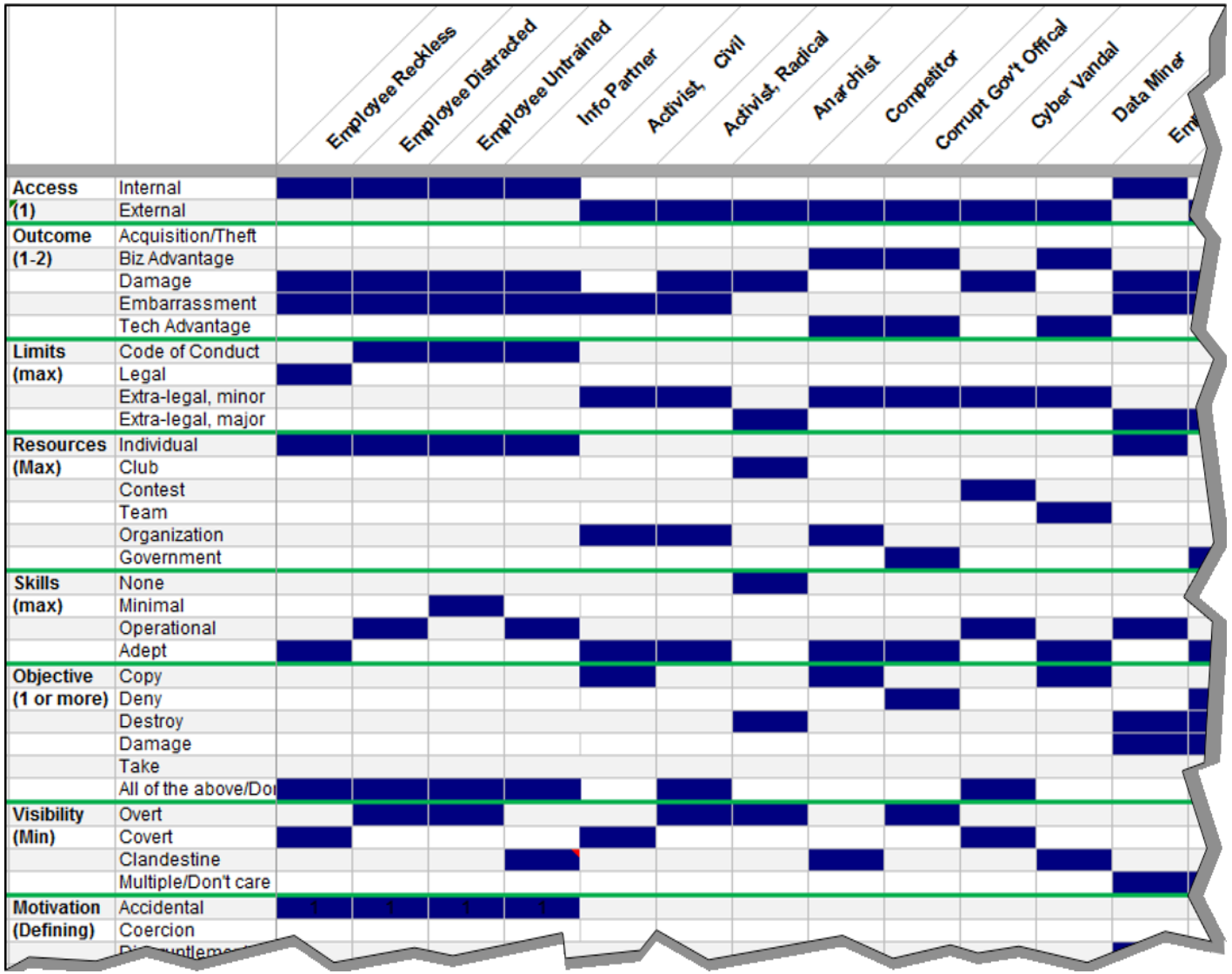
Threat Agent Risk Assessment

- Identify the most likely attackers, targets, and methods
- Consider accepted levels of risk and current controls
- Determine the most critical exposures
- Complementary to traditional ways of analyzing security risks

‘Interesting’ Threat Agents



Example Threat Agent Library



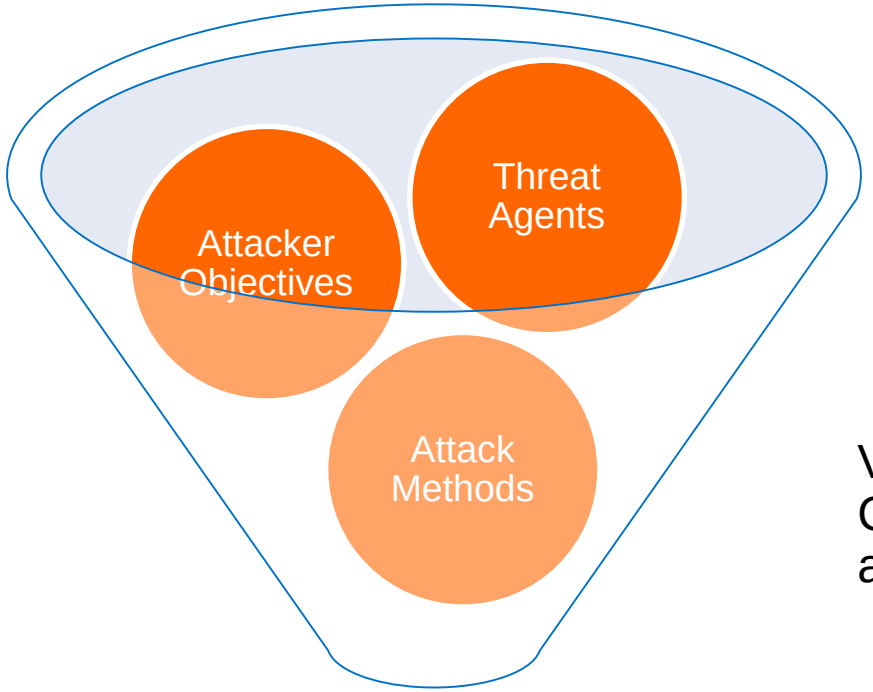
Threat Archetypes

Relevant Attributes

The Intel Threat Agent Library example is available at communities.intel.com

Threat Agent Methodology

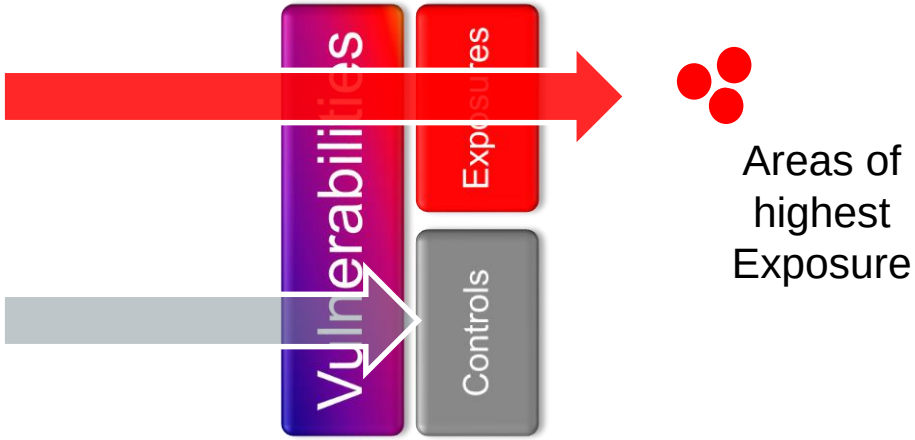
Distilling the Threats



All possible Threats, Objectives, and Methods

Vulnerabilities without Controls for these attacks are likely Exposures

Highest risk Threats, Objectives, and Methods

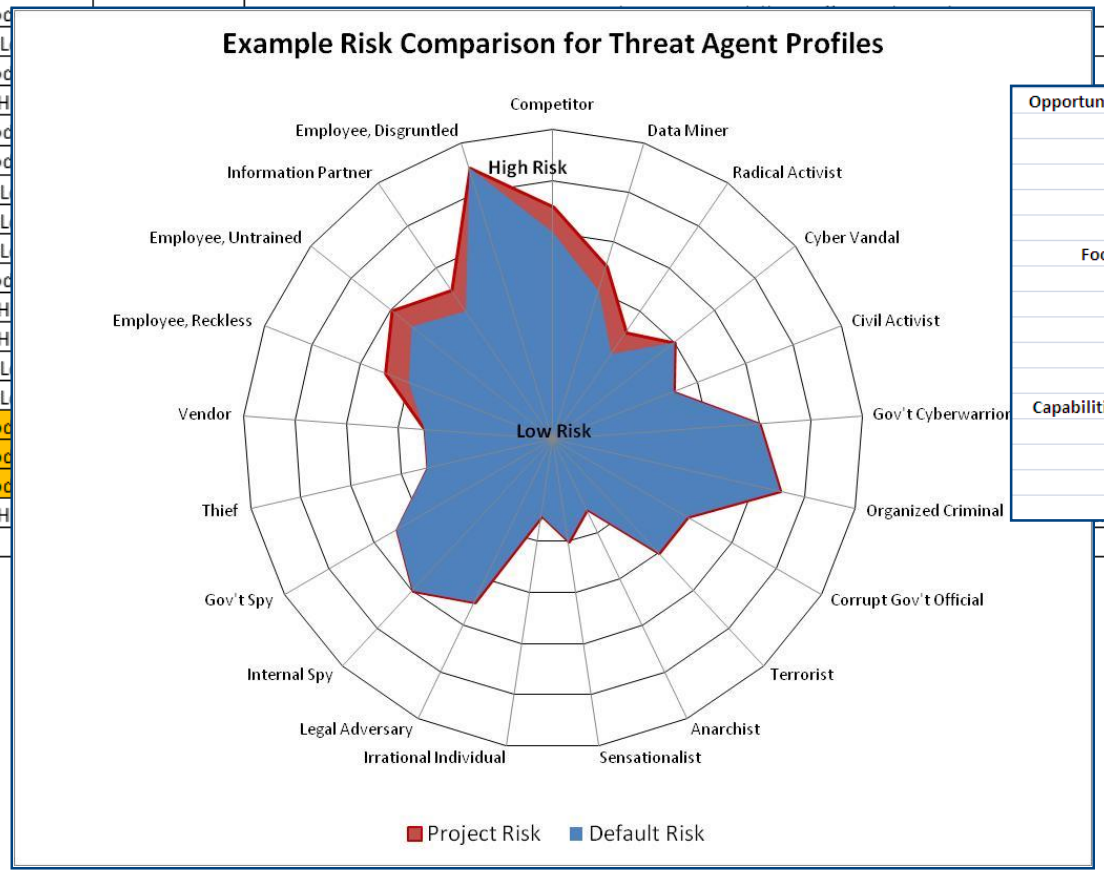


Areas of highest Exposure

Communicating Risks of Threat Agents

Threat Agent Risk Assessment (TARA) for: *Example Project*

Threat Agents	Default Risk	Project Risk	Delta Risk	Risk Evaluation Rational	Intel Risk: Opportunity	Focus	Capabilities	3 to 12	IQC Risk: Opportunity	Focus	Capabilities	3 to 12
Competitor	Moderate	High	Increased	May have increased access to the ICQ devices as well as opportunities to stealthily attempt compromises	1	4	3	8	1	4	4	9
Data Miner	Moderate	Moderate	Increased	TA has much greater opportunities if IQC is used on a system compromised by the TA	1	2	3	6	1	2	4	7
Radical Activist	Low	Moderate	Increased	IQC represents an opportunity to achieve objectives, in alignment with skills, resources, and limits	1	1	2	4	1	1	3	5
Cyber Vandal	Moderate	Mod			1	3	2	6	1	3	2	6
Civil Activist	Low	L			1	1	2	5	1	1	2	5
Gov't Cyberwarrior	Moderate	Mod			2	2	4	8	2	2	4	8
Organized Criminal	High	H										9
Corrupt Gov't Official	Moderate	Mod										6
Terrorist	Moderate	Mod										6
Anarchist	Low	L										3
Sensationalist	Low	L										4
Irrational Individual	Low	L										3
Legal Adversary	Moderate	Mod										7
Internal Spy	High	H										8
Gov't Spy	High	H										7
Thief	Low	L										5
Vendor	Low	L										5
Employee, Reckless	Moderate	Mod										7
Employee, Untrained	Moderate	Mod										8
Information Partner	Moderate	Mod										7
Employee, Disgruntled	High	H										11
Ex-employee w/access, disgruntled*	N/A											0



Opportunity		
	1	No Trust - External
	2	Partial Trust - Partner (or would likely leverage a partner/insider)
	3	Basic Trust - Internal
	4	High Trust - Admin
Focus		
	1	Indirect - Targets of opportunity
	2	Blended - Preferred targets of opportunity
	3	Direct - Opportunities at a target
	4	Specific - Opportunities for specific objectives at a target
Capabilities		
	1	Low - Individual, basic skills
	2	Intermediate - General skills, collaboration
	3	High - Professional skills, formal teamwork
	4	Exceptional - Superior skills, professional program management

Two types of victims exist: those with something of value and those who are easy targets

Therefore: Don't be an easy target, and protect your valuables

Bad Assumptions & Good Practices

Bad Assumptions:

- I am not a target for attack ->
  Where there is value, there is risk. …(the Willie Sutton principle)
- Security is an IT/user/security/product/other-guy problem ->
  It is everyone's problem and requires everyone to contribute.
- Closed environments ->
  …aren't really as closed as you think.
- Insiders aren't a major problem ->
  Insiders are a significant risk, but largely hidden until something big goes wrong!

Bad Assumptions & Good Practices

Good Practices:

- Understand primary threats (most relevant agents, their objectives, & likely methods)
- Value and grow security savvy users/employees
- Plan across the Defense-in-Depth (predict, prevent, detect, respond)
- Disrupt the attack cycle (threat agent -> methods -> objectives)
- Think ahead, but never forsake security fundamentals
- Gauge investments with Security Aspects (innovative, hardened, trusted, ubiquitous)

Criteria for Good Choices in Technology and Security

Smart

Innovation to deliver more capable solutions to keep pace with threats

Trusted

Well designed, built, and tested solutions backed by commitment, reputation, and expertise

Strong

Hardened, embedded, and faster technology, resistant to compromise

Ubiquitous

Security benefitting all users and devices across the compute landscape

Conclusion

- Leadership is crucial
- Seek an optimal level of security
- Leverage home-field advantage, implement industry best-known-methods
- Know your threats, assets, controls, and exposures
- Treat security as a continuous cycle
- Stay positive, keep learning, and share with the community


intel
Security