ISACA®

Trust in, and value from, information systems

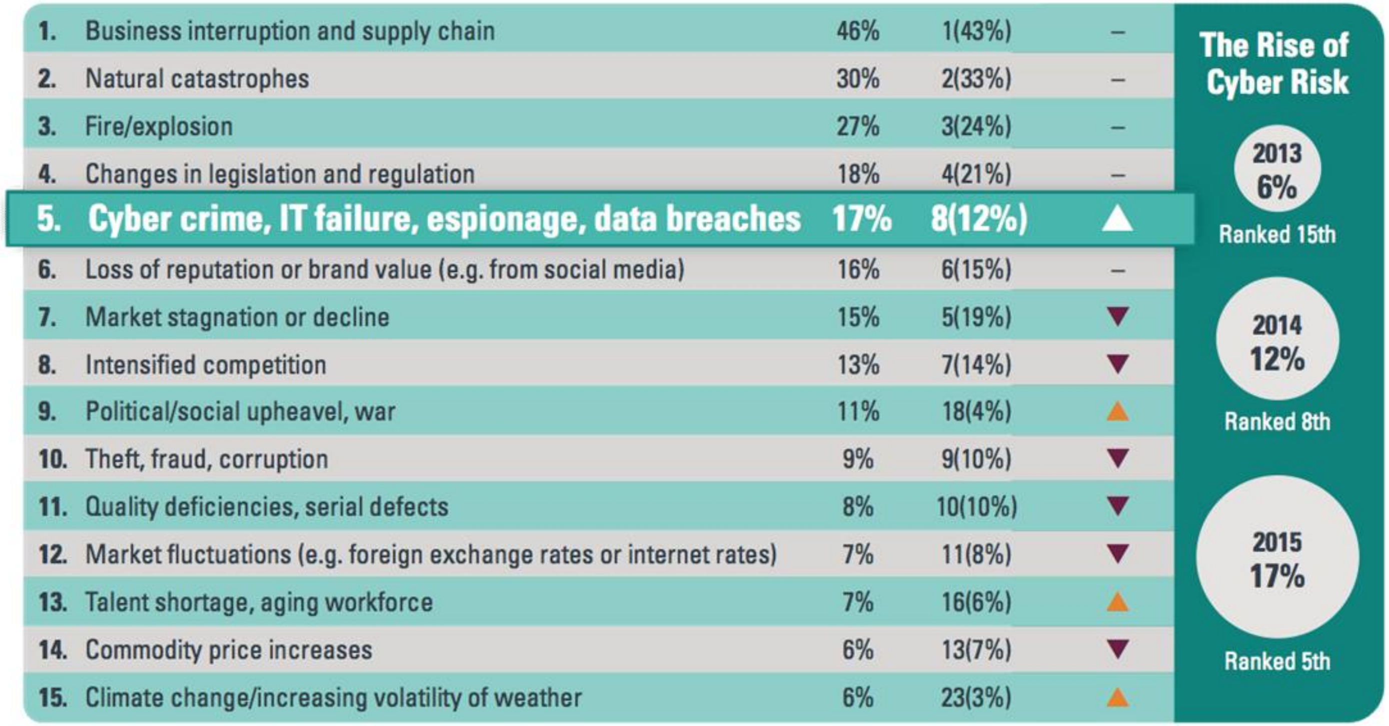
COLLECTIVE DEFENCE AND THE USE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Leonard Ong, CISA, CISM, CRISC, CGEIT, CoBIT 5 Implementer & Assessor

21 September 2016

CYBER
ATTACKS
AHEAD

CYBERSECURITY HAS BECOME A STRATEGIC RISK



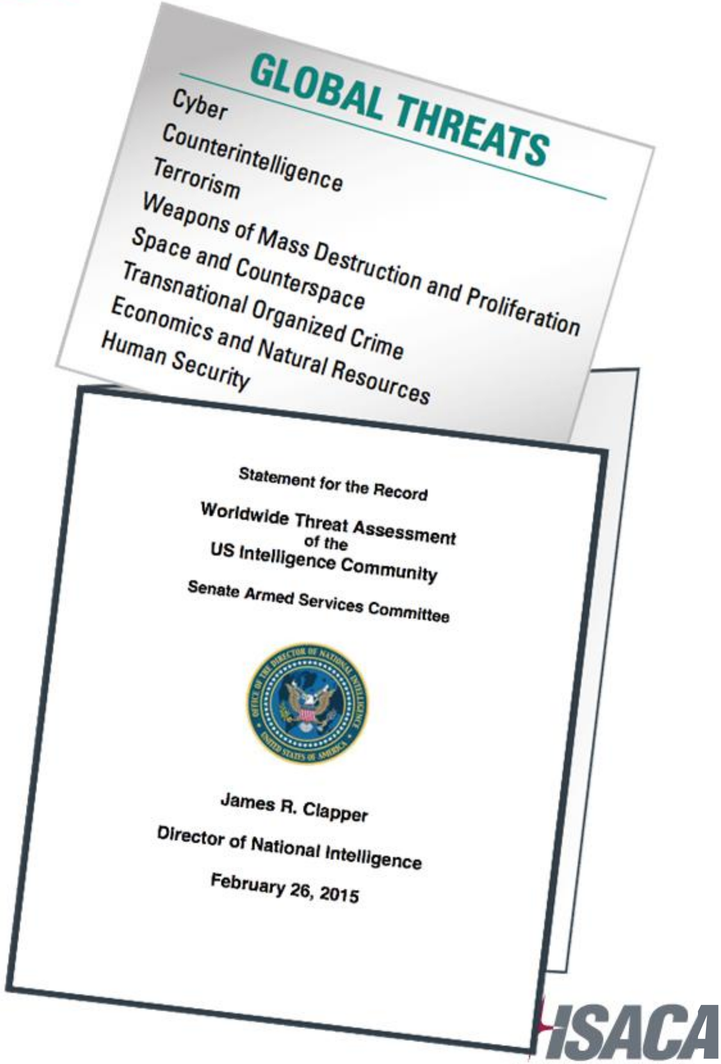
1.	Business interruption and supply chain	46%	1(43%)	–
2.	Natural catastrophes	30%	2(33%)	–
3.	Fire/explosion	27%	3(24%)	–
4.	Changes in legislation and regulation	18%	4(21%)	–
5.	**Cyber crime, IT failure, espionage, data breaches**	**17%**	**8(12%)**	▲
6.	Loss of reputation or brand value (e.g. from social media)	16%	6(15%)	–
7.	Market stagnation or decline	15%	5(19%)	▼
8.	Intensified competition	13%	7(14%)	▼
9.	Political/social upheavel, war	11%	18(4%)	▲
10.	Theft, fraud, corruption	9%	9(10%)	▼
11.	Quality deficiencies, serial defects	8%	10(10%)	▼
12.	Market fluctuations (e.g. foreign exchange rates or internet rates)	7%	11(8%)	▼
13.	Talent shortage, aging workforce	7%	16(6%)	▲
14.	Commodity price increases	6%	13(7%)	▼
15.	Climate change/increasing volatility of weather	6%	23(3%)	▲

The Rise of Cyber Risk

2013
6%
Ranked 15th

2014
12%
Ranked 8th

2015
17%
Ranked 5th



GLOBAL THREATS

Cyber
Counterintelligence
Terrorism
Weapons of Mass Destruction and Proliferation
Space and Counterspace
Transnational Organized Crime
Economics and Natural Resources
Human Security

Statement for the Record

Worldwide Threat Assessment
of the
US Intelligence Community

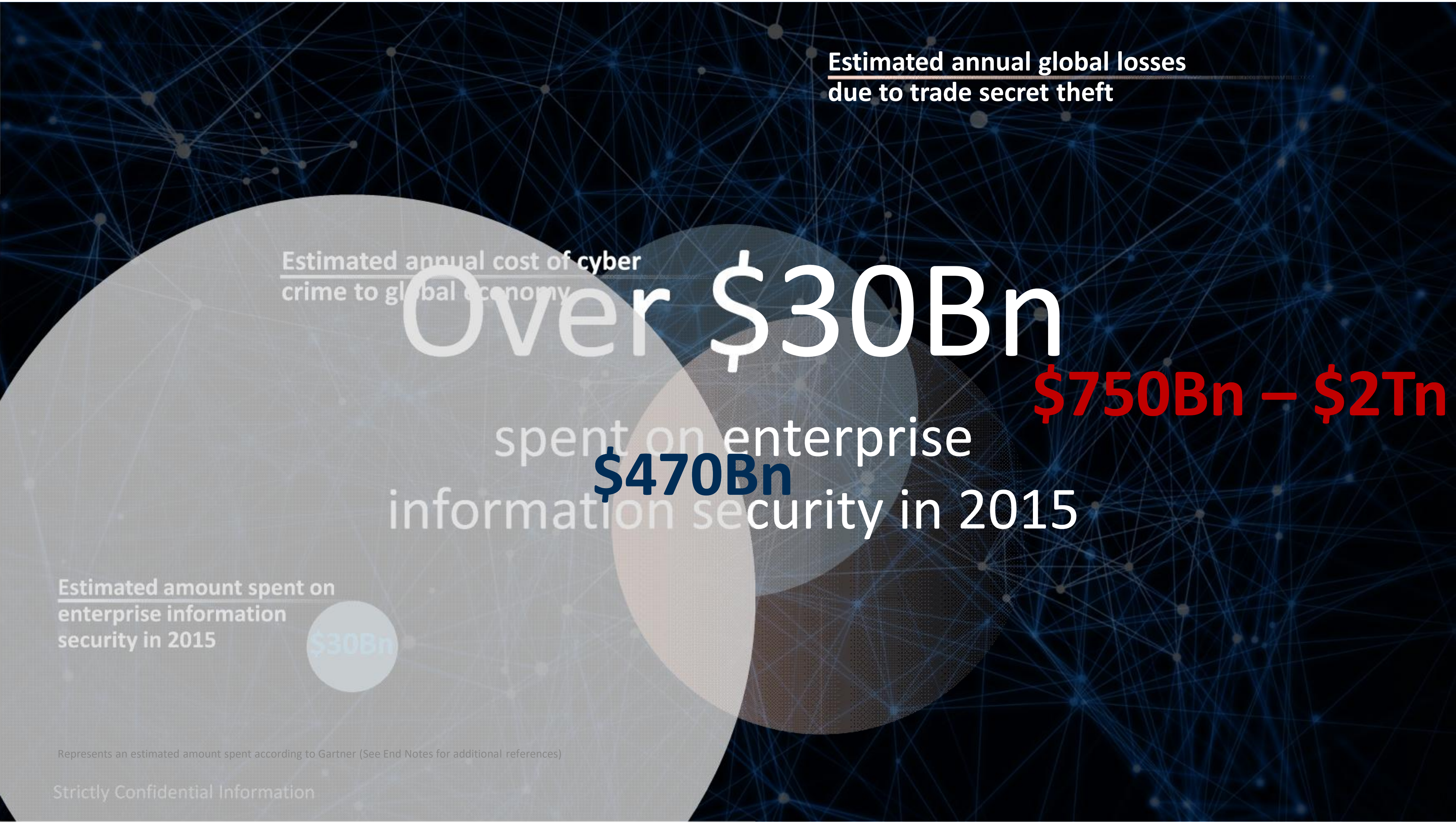
Senate Armed Services Committee

James R. Clapper

Director of National Intelligence

February 26, 2015

Cybersecurity is Now
Considered a Critical Risk by
Boards & National Leaders



Over $30Bn spent on enterprise information security in 2015

Estimated annual global losses due to trade secret theft

$750Bn – $2Tn

Estimated annual cost of cyber crime to global economy

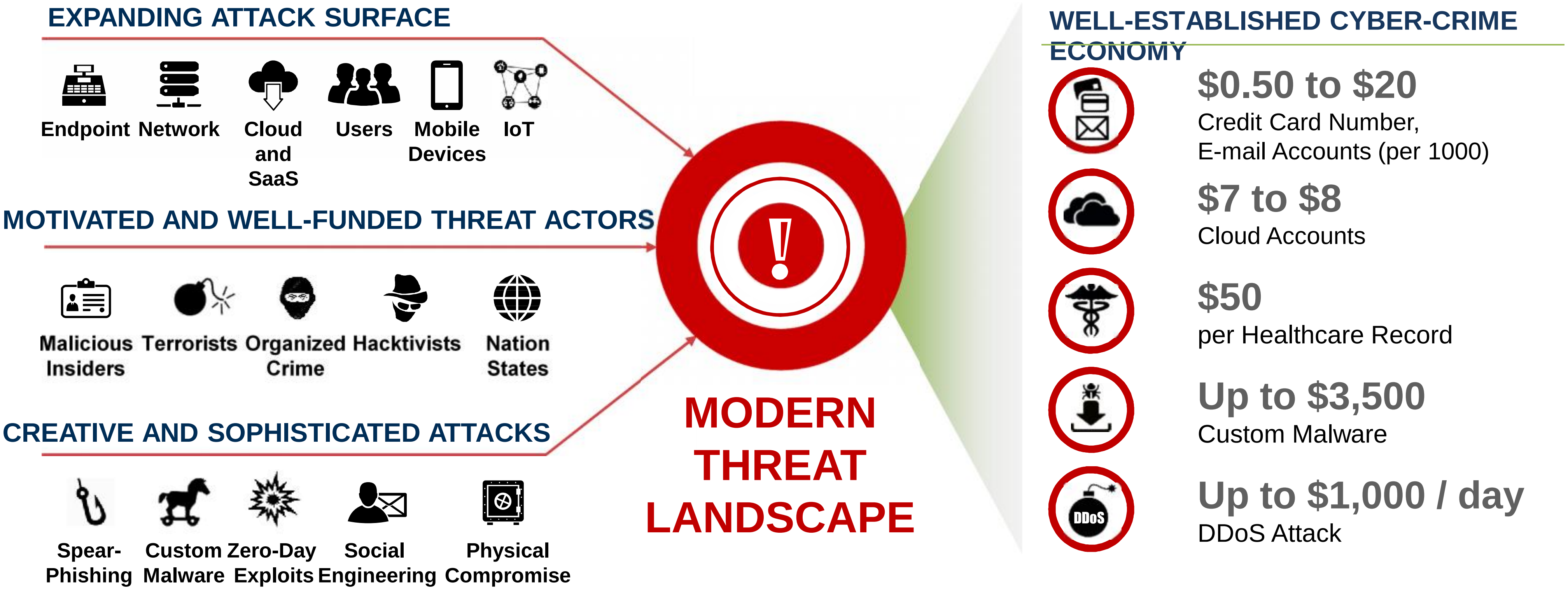
$470Bn

Estimated amount spent on enterprise information security in 2015

$30Bn

Represents an estimated amount spent according to Gartner (See End Notes for additional references)

THE MODERN CYBER THREAT PANDEMIC



EXPANDING ATTACK SURFACE

Endpoint, Network, Cloud and SaaS, Users, Mobile Devices, IoT

MOTIVATED AND WELL-FUNDED THREAT ACTORS

Malicious Insiders, Terrorists, Organized Crime, Hacktivists, Nation States

CREATIVE AND SOPHISTICATED ATTACKS

Spear-Phishing, Custom Malware, Zero-Day Exploits, Social Engineering, Physical Compromise

MODERN THREAT LANDSCAPE

WELL-ESTABLISHED CYBER-CRIME ECONOMY

$0.50 to $20
Credit Card Number,
E-mail Accounts (per 1000)

$7 to $8
Cloud Accounts

$50
per Healthcare Record

Up to $3,500
Custom Malware

Up to $1,000 / day
DDoS Attack

Source Symantec, Underground black market: Thriving trade in stolen data, malware, and attack services. December 10, 2014; Medscape, Stolen EHR Charts Sell for $50 Each on Black Market, April 28, 2014

Prevention-Centric Approaches are Insufficient

Prevention-Centric Approaches

- Firewalls
- Intrusion Prevention Systems
- Anti-Virus/Malware
- Sandboxing

Preventable Threats

- Previously Seen
- Signature-Based
- Static
- One-Dimensional

205

Median number of days that companies were compromised before detection of threat

- Mandiant M-Trends 2015

Modern Cyber Threats

- Advanced
- Stealthy
- Persistent
- Dynamic
- Multi-Dimensional

INSIDERS CONTINUE TO POSE A THREAT

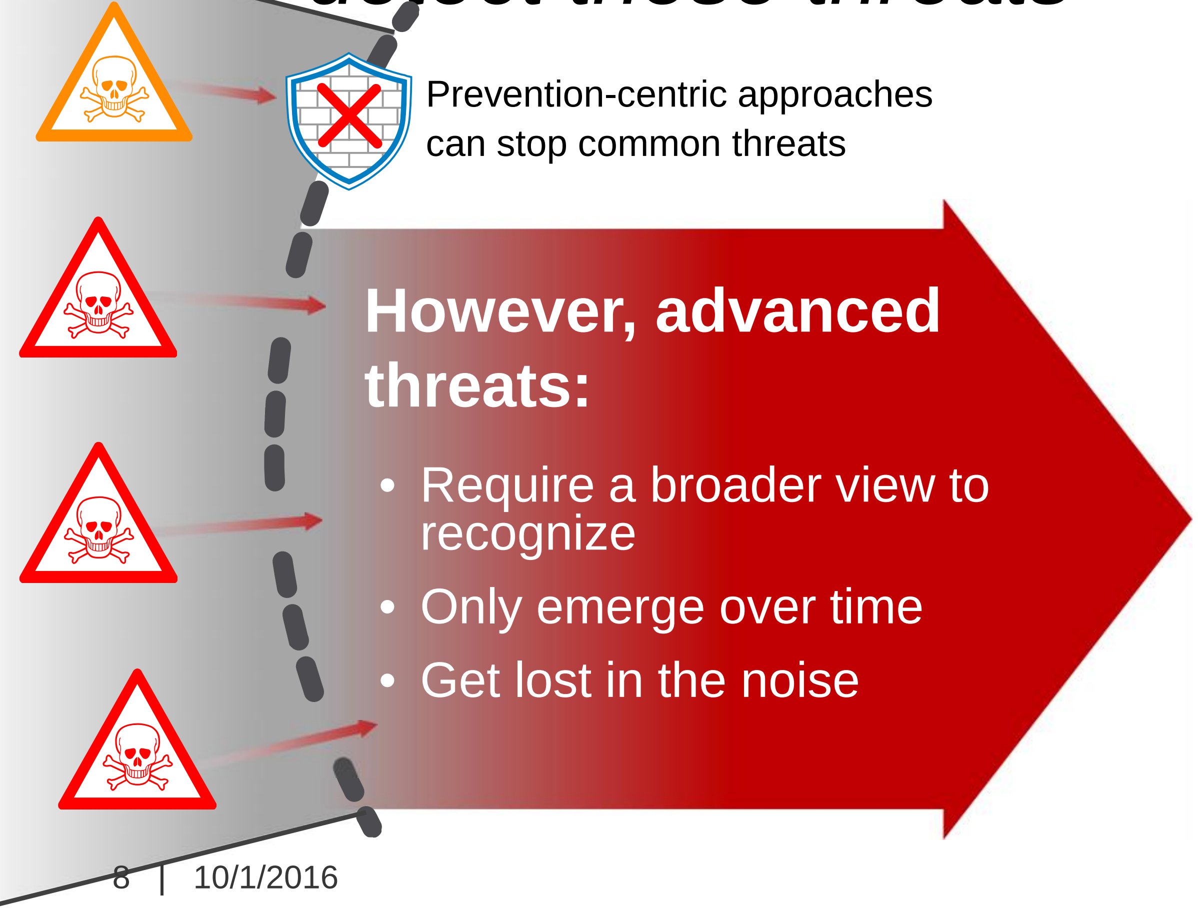
- Data security and insider threats continue to be a challenge particularly as mobility brings complexity to risk management
- Motivations range from financial to fun
- Theft, manipulation of data, data destruction are all fair gamea
- Reputation can also become the target

“Insider involvement in 32% of claims submitted (to insurers)”
2015 NetDiligence Cyber Claims Study

“89% feel at least somewhat vulnerable to insider attacks”
2015 Vormetric Insider Threat Report

A NEW SECURITY APPROACH IS REQUIRED

Analytics with Artificial Intelligence *can best detect these threats*



Prevention-centric approaches can stop common threats

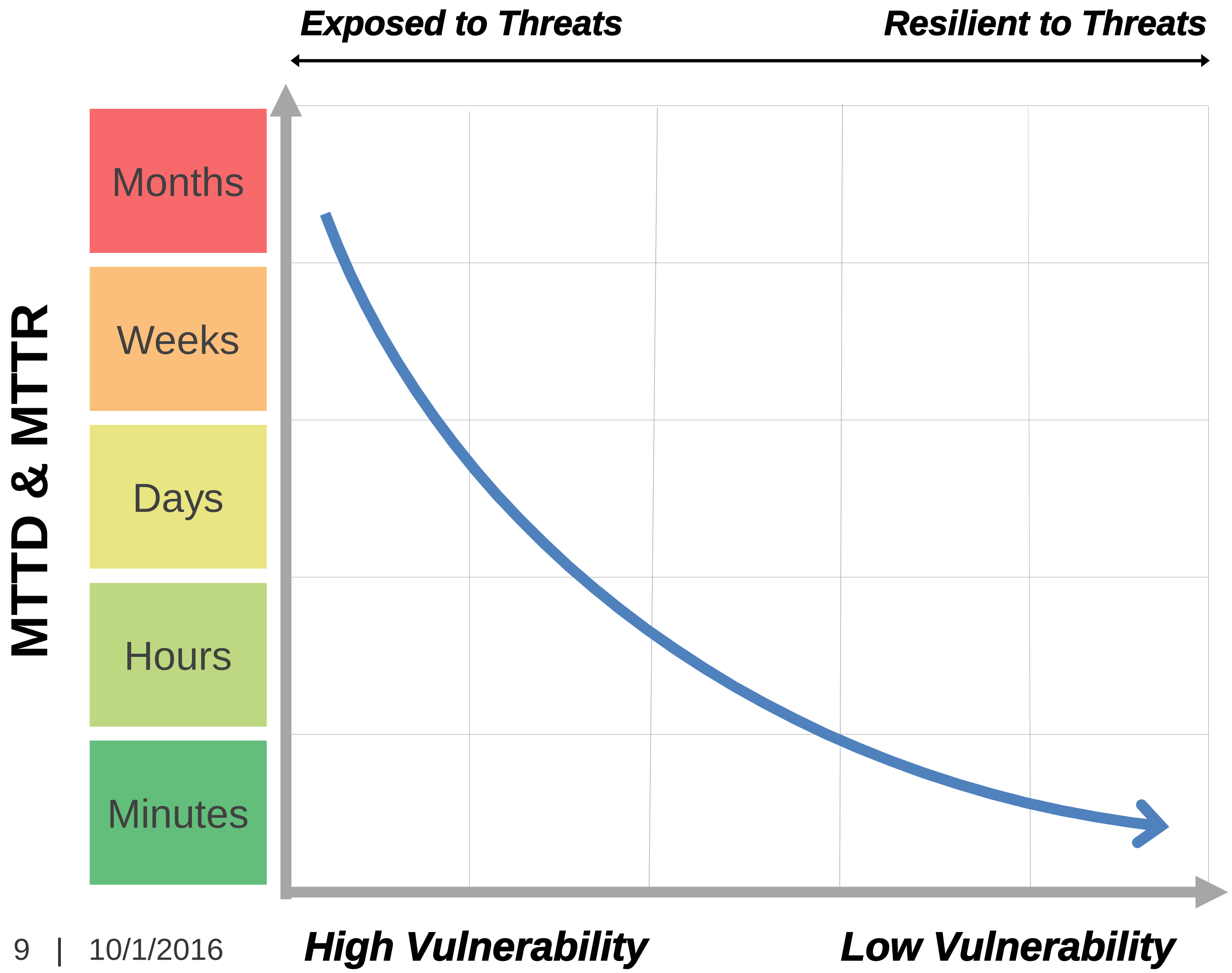
However, advanced threats:

- Require a broader view to recognize
- Only emerge over time
- Get lost in the noise

The needs:

- Machine learning & AI to identify advanced threats
- Qualified and prioritized detection, reducing noise
- Adaptive Incident response workflow orchestration and automation
- Capabilities to prevent high-impact breaches & damaging cyber incidents

FASTER DETECTION & RESPONSE REDUCES RISK



MEAN-TIME-TO-DETECT (MTTD)
The average time it takes to recognize a threat requiring further analysis and response efforts

MEAN-TIME-TO-RESPOND (MTTR)
The average time it takes to respond and ultimately resolve the incident

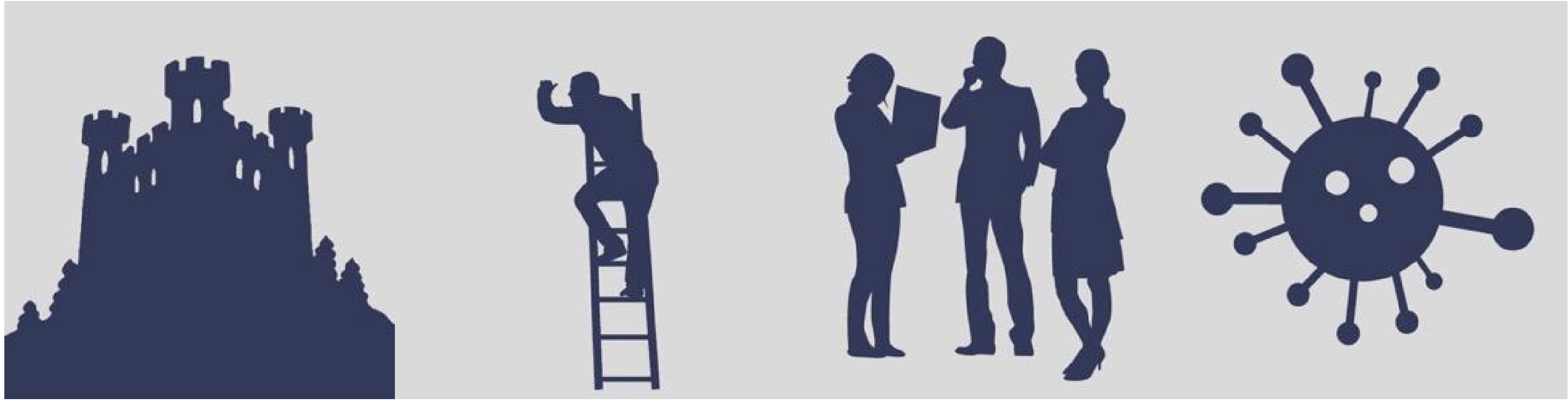
As organizations improve their ability to quickly detect and respond to threats, the risk of experiencing a damaging breach is greatly reduced

ISACA®

Trust in, and value from, information systems

ARTIFICIAL INTELLIGENCE

THE NEED FOR ARTIFICIAL INTELLIGENCE / MACHINE LEARNING



It is impossible to fully secure your enterprise network

Sophisticated threats will always find a way in

Insider threat is as important as external

It is impossible to keep rules & signatures up to date 24/7

WHY IS THE ENTERPRISE IMMUNE SYSTEM UNIQUE?

Learns ‘self’
For every individual user, device and network, using unsupervised machine learning

Detects insider & external threats
That bypass traditional security tools

Real time
Continually identifies anomalies, as they emerge

100% visibility
Visualizes entire network, auto-classifies threats and allows for in-depth investigations

Play-back
Analyzes and correlates events over time. Ability to replay incidents

MACHINE LEARNING & MATHEMATICS

- Advanced Bayesian mathematics pioneered at the University of Cambridge
- Recursive Bayesian Estimation detects subtle changes within data series in real time and adaptively iterates its models
- Numerous approaches used to classify the probability of an action based on previous and emerging behaviours
- No ‘a priori’ assumptions about good or bad – mathematical models are unique to your organisation
- Distribution is built from a complex set of low-level host, network and traffic observations or ‘features’

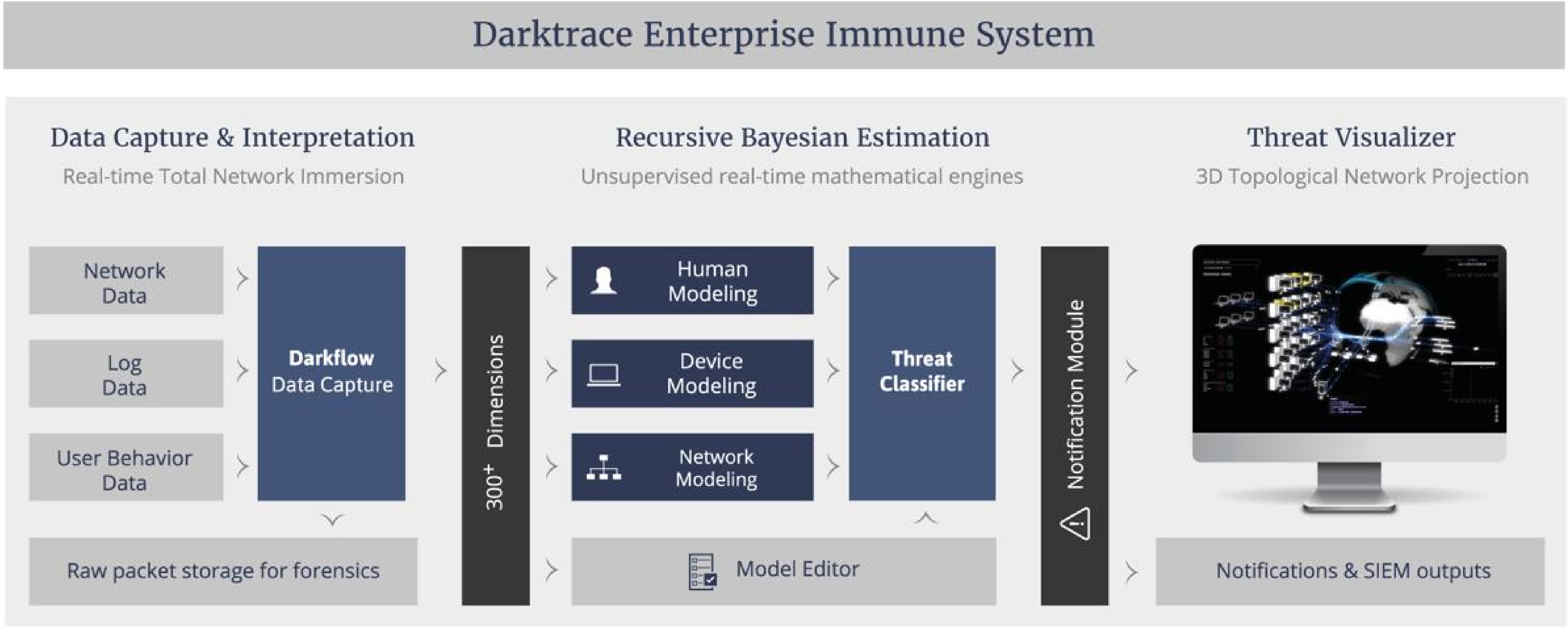
UNIVERSITY OF CAMBRIDGE

$$P(\boldsymbol{\theta}_k|\mathbf{D},\mathcal{M}_k) = \frac{P(\mathbf{D}|\boldsymbol{\theta}_k,\mathcal{M}_k)\,P(\boldsymbol{\theta}_k \mid \mathcal{M}_k)}{P(\mathbf{D} \mid \mathcal{M}_k)}$$

$$P(\mathbf{D} \mid \mathcal{M}_k) = \int P(\mathbf{D} \mid \boldsymbol{\theta}_k,\mathcal{M}_k)P(\boldsymbol{\theta}_k \mid \mathcal{M}_k)\,d\boldsymbol{\theta}_k.$$

$$P(\mathcal{M}_k \mid \mathbf{D}) \propto P(\mathbf{D} \mid \mathcal{M}_k)P(\mathcal{M}_k),$$

TECHNOLOGY ARCHITECTURE EXAMPLE - DARKTRACE



Darktrace Enterprise Immune System

Data Capture & Interpretation

Real-time Total Network Immersion

Recursive Bayesian Estimation

Unsupervised real-time mathematical engines

Threat Visualizer

3D Topological Network Projection

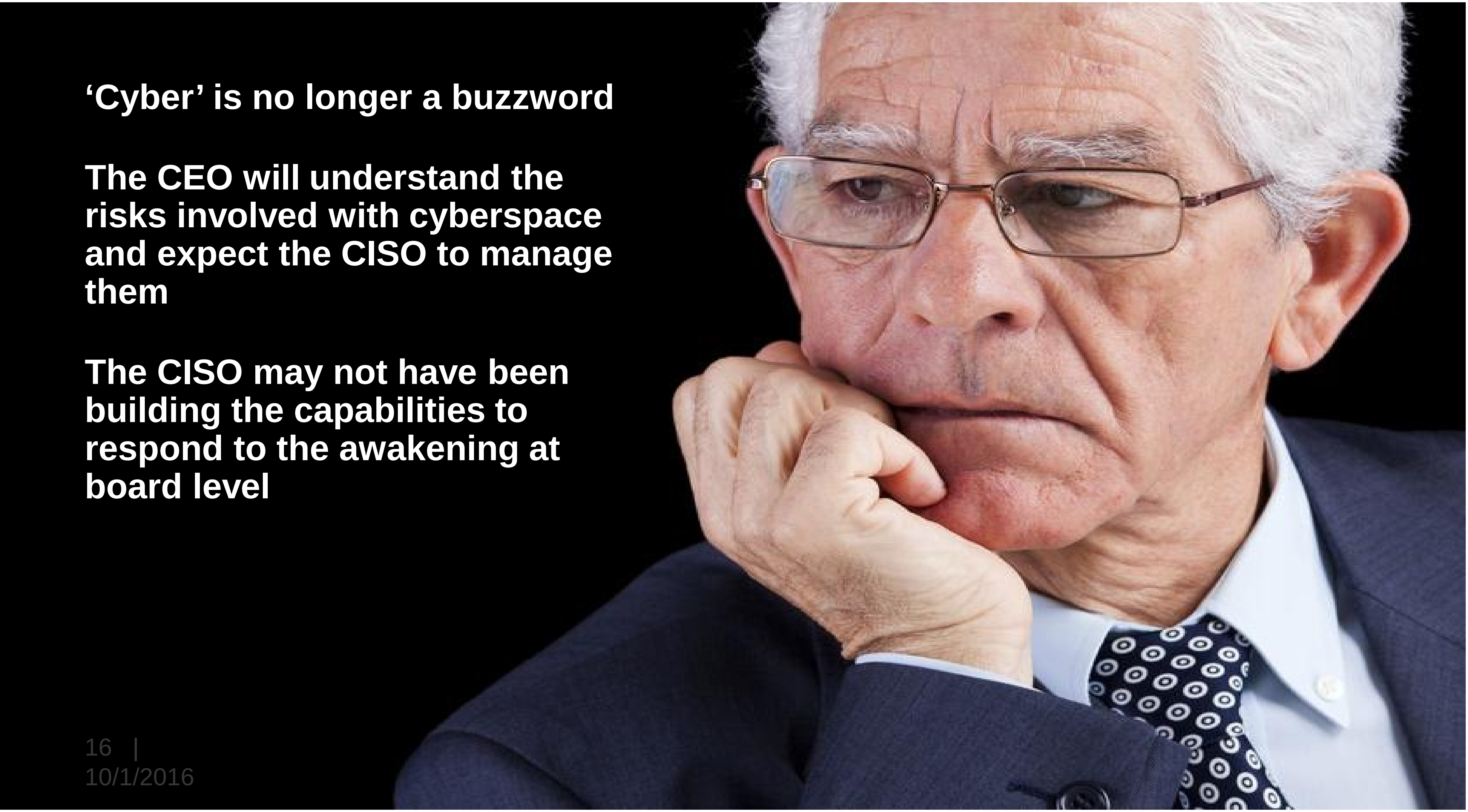
Trust in, and value from, information systems

ISACA®

Trust in, and value from, information systems

COLLECTIVE DEFENSE

THE CEO GETS IT, NOW YOU HAVE TO DELIVER



‘Cyber’ is no longer a buzzword

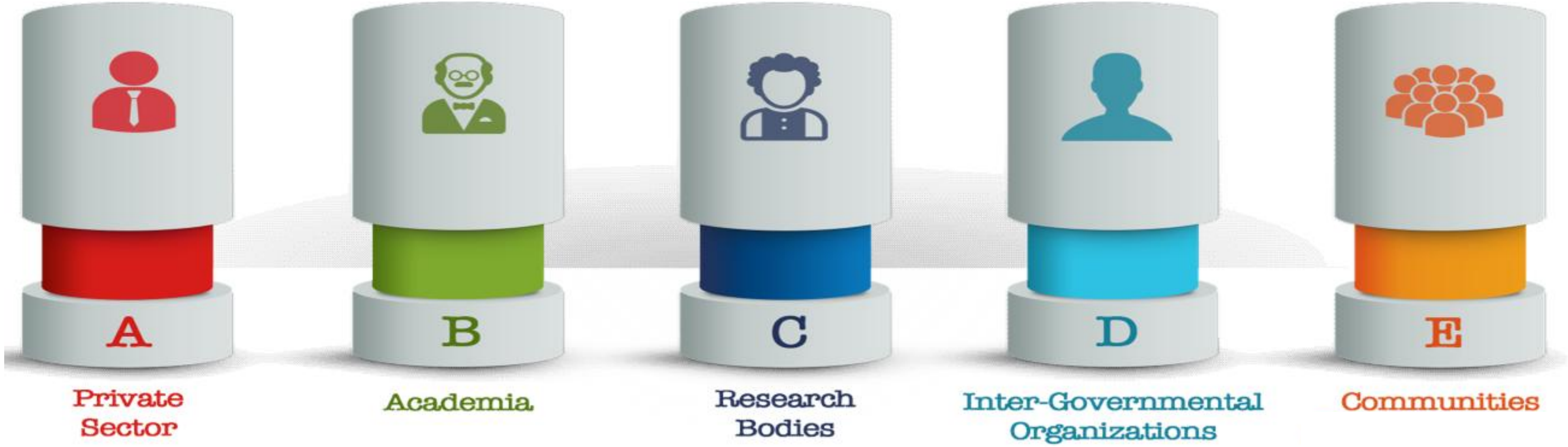
The CEO will understand the risks involved with cyberspace and expect the CISO to manage them

The CISO may not have been building the capabilities to respond to the awakening at board level

THE BENEFITS OF COLLECTIVE DEFENSE

- Sharing of Critical Resources
- Eliminating Wasteful Redundancy
- Building Better Legal Defensibility
- Leveraging Size and Scale For Purchasing Power
- Greater Ability to Influence Vendor Community
- Increasing Collective Institutional Knowledge

Multi-Stakeholder Approach



HEALTHCARE CISO GROUP

•75 security leaders of the largest healthcare companies in the world

•Meet semiannually, calls monthly, and email/portal sharing

•Primary focus is on security strategy, polciy & sharing best practices

•Benchmarking exercises to compare maturity within sector and among sectors

•Partner with McKinsey for education awareness of senior business executives & government officials

•No charge to members

Cleveland Clinic
REGENERON
Abbott
Lilly
GILEAD
BAYLOR
MERCYHEALTH
BD
GE Healthcare
biogen idec
KAISER PERMANENTE
Blue Cross Blue Shield of Michigan
Baxter
Pfizer
HIGHMARK
Johnson & Johnson
TENET
CATHOLIC HEALTH INITIATIVES
HCA
EXPRESS SCRIPTS
BIOMET
Celgene
Horizon
MERCK
AMGEN
JOHNS HOPKINS
Florida Blue
aetna
Boehringer Ingelheim
McKESSON
Edwards
gsk
EmblemHealth
Actavis
MOLINA HEALTHCARE
MONSANTO
ALLERGAN
AmerisourceBergen
zimmer
SANOFI
AstraZeneca
Bristol-Myers Squibb
CMS
PHILIPS
QUINTILES

ISACA®
Trust in, and value from, information systems

INFORMATION SHARING AND ANALYSIS CENTRES

Auto ISAC

Aviation ISAC

Communications ISAC

Defense Industrial Base ISAC

Downstream Natural Gas ISAC

Electricity ISAC

Emergency Management & Response ISAC

Financial Services ISAC

Information Technology ISAC

Maritime ISAC

Multi-State ISAC

INFORMATION SHARING AND ANALYSIS CENTRES

National Health ISAC

Oil and Natural Gas ISAC (ONG)

Over the Road & Motor Coach ISAC

Public Transit ISAC

Real Estate ISAC

Research and Education ISAC

Retail ISAC

Supply Chain ISAC

Surface Transportation ISAC

Water ISAC

INFORMATION SHARING & ANALYSIS TOOLS

Threat Data, Information Sharing

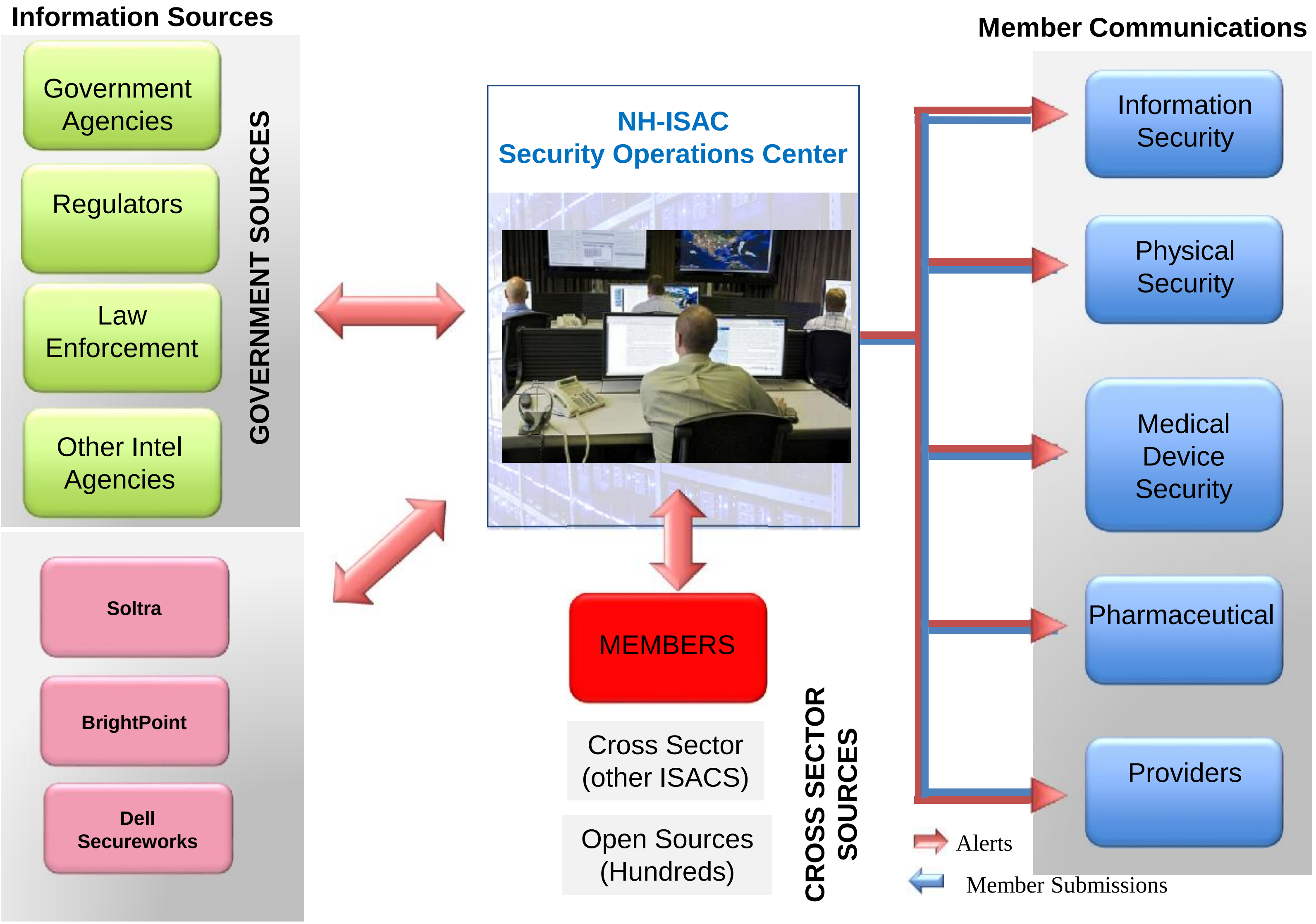
- Anonymous Submissions
- Amber Listserver
- Relevant/Actionable Cyber & Physical Alerts
- Special Interest Group List Servers
- Document Repository
- Member Surveys
- Cyber Utility
- Security Automation
- Threat Viewpoints

Ongoing Engagement

- Threat Calls
- Emergency Member Calls
- Semi-Annual Member Meetings and Conferences
- Regional Outreach Program
- Educational Webinars

Readiness Exercises

- Sector/Intra-Sector Exercises
- Cross-Sector Exercises
  - CyberStorm V
  - OCF
  - GridEX



Information Sources

Government Agencies

Regulators

Law Enforcement

Other Intel Agencies

GOVERNMENT SOURCES

Soltra

BrightPoint

Dell Secureworks

NH-ISAC
Security Operations Center

MEMBERS

Cross Sector (other ISACS)

Open Sources (Hundreds)

CROSS SECTOR SOURCES

Member Communications

Information Security

Physical Security

Medical Device Security

Pharmaceutical

Providers

🟥 Alerts

🟦 Member Submissions

INFORMATION SHARING: TRAFFIC LIGHT PROTOCOL

🔴 ⦿Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group

🟡 ⦿This information may be shared with ISAC members.

🟢 ⦿Information may be shared with ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums

⚪ ⦿This information may be shared freely and is subject to standard copyright rules

TYPES OF INFORMATION SHARED

Cyber Threats, Vulnerabilities, Incidents

✓Malicious Sites

✓Threat Actors, Objectives

✓Threat Indicators

✓TTPs, Observables

✓Courses of Action

✓Exploit Targets

✓Denial of Service Attacks

✓Malicious Emails: Phishing/ Spearphishing

✓Software Vulnerabilities

✓Malicious Software

✓Analysis and risk mitigation

✓Incident response

SAMPLE OF ISAC SHARING

Indicators of Compromise
IP Address, Subject Line, MD5, TTP, Malware

Ask a question
Anyone else seeing?...
What do you do in this situation?....
How do you handle?…………*mobile device management*

Share a Best Practice
Here’s how we……

Share a Mitigation Strategy
Here’s a script you can use……*MIFR*
We did this……

A COMMON LANGUAGE

Structured Threat Information Expression is a common language a way for all to speak the same

Trusted Automated eXchange of Indicator Information (TAXII)

- **The goal of TAXII is to facilitate the exchange of structured cyber threat information**

- **TAXII is a protocol over which STIX can be transported**

WHAT IS CYBER THREAT INTELLIGENCE?
8 CONSTRUCTS OF STIX

Atomic

Observable

What threat activity are we seeing?

Tactical

Indicator

What threats should I look for on my networks and systems and why?

Operational

Incident

Where has this threat been seen?

Course of Action

What can I do about it?

ExploitTarget

What weaknesses does it exploit?

Strategic

ThreatActor

Who is responsible for this threat?

Campaign

Why do they do this?

TTP

What do they do?

THANK YOU