A CORPORATE GUIDE TO SURVIVING CYBERWARFARE THROUGH CYBER RESILIENCY

Dr. John D. Johnson, CISSP, CRISC

CEO/Founder Aligned Security

9 October 2017 • Atlanta, GA

Hacker | Halted

Defining Resilience

About 10,600,000 results (0.97 seconds)

re·sil·ience
/rəˈzilyəns/

noun
noun: **resiliency**

1. the capacity to recover quickly from difficulties; toughness.
   "the often remarkable resilience of so many British institutions"
2. the ability of a substance or object to spring back into shape; elasticity.
   "nylon is excellent in wearability and resilience"

Cyber Resilience is an evolving perspective that is rapidly gaining recognition. The concept essentially brings the areas of information security, business continuity and (organizational) **resilience** together.

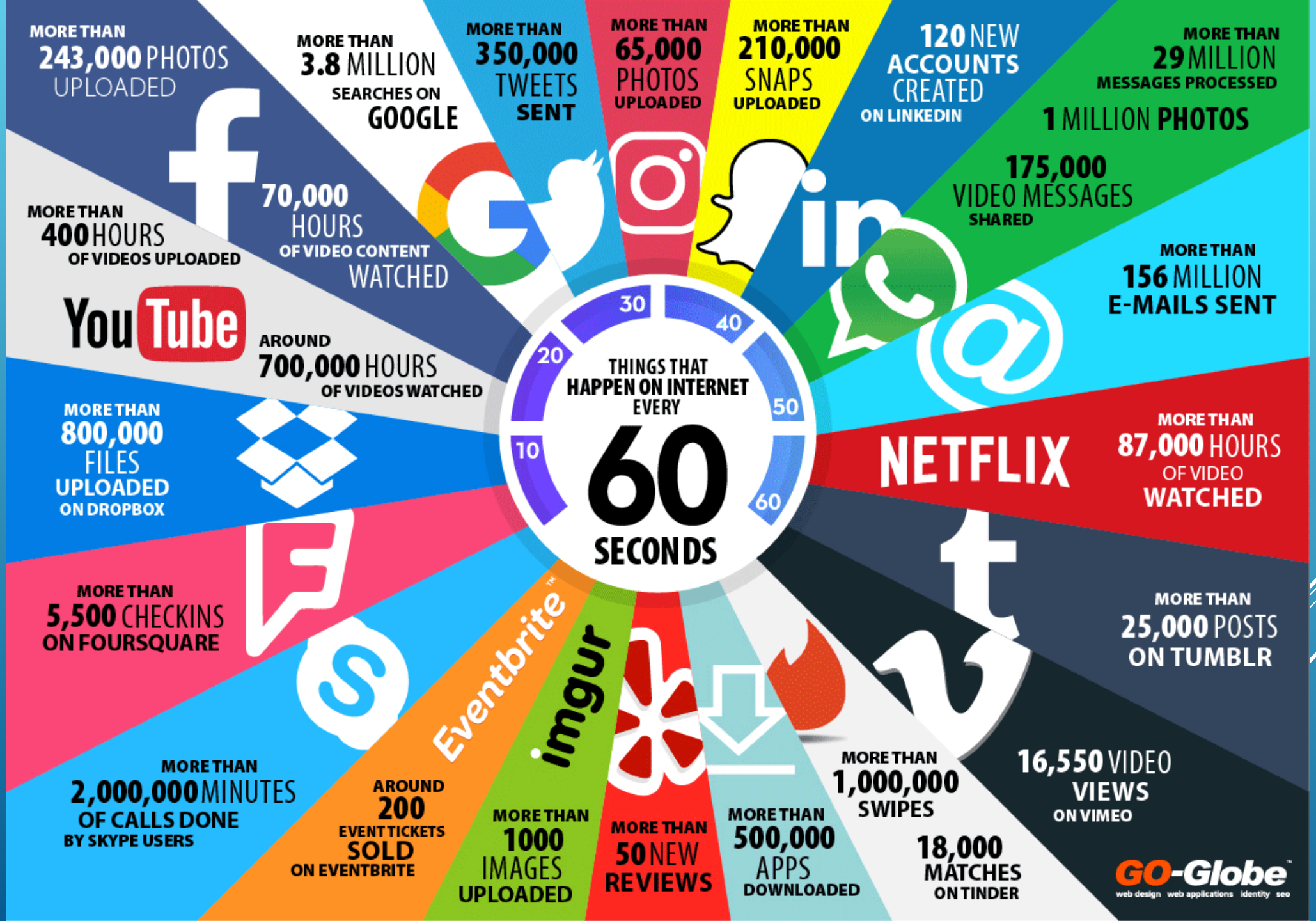
Cyber Resilience - Wikipedia
https://en.wikipedia.org/wiki/Cyber_Resilience

Yesterday


In the past a castle model of defense was
adequate to keep the adversaries at bay


IBM
System 360

Today


MORE THAN 243,000 PHOTOS UPLOADED
MORE THAN 3.8 MILLION SEARCHES ON GOOGLE
MORE THAN 350,000 TWEETS SENT
MORE THAN 65,000 PHOTOS UPLOADED
MORE THAN 210,000 SNAPS UPLOADED
120 NEW ACCOUNTS CREATED ON LINKEDIN
MORE THAN 29 MILLION MESSAGES PROCESSED
1 MILLION PHOTOS
175,000 VIDEO MESSAGES SHARED
MORE THAN 156 MILLION E-MAILS SENT
70,000 HOURS OF VIDEO CONTENT WATCHED
MORE THAN 400 HOURS OF VIDEOS UPLOADED
YouTube
AROUND 700,000 HOURS OF VIDEOS WATCHED
THINGS THAT HAPPEN ON INTERNET EVERY 60 SECONDS
10
20
30
40
50
60
MORE THAN 800,000 FILES UPLOADED ON DROPBOX
NETFLIX
MORE THAN 87,000 HOURS OF VIDEO WATCHED
MORE THAN 5,500 CHECKINS ON FOURSQUARE
MORE THAN 25,000 POSTS ON TUMBLR
MORE THAN 2,000,000 MINUTES OF CALLS DONE BY SKYPE USERS
AROUND 200 EVENT TICKETS SOLD ON EVENTBRITE
Eventbrite
imgur
MORE THAN 1000 IMAGES UPLOADED
MORE THAN 50 NEW REVIEWS
MORE THAN 500,000 APPS DOWNLOADED
MORE THAN 1,000,000 SWIPES
18,000 MATCHES ON TINDER
16,550 VIDEO VIEWS ON VIMEO
GO-Globe
web design web applications identity seo

Consumer & Home

Smart Infrastructure

Security & Surveillance

Healthcare

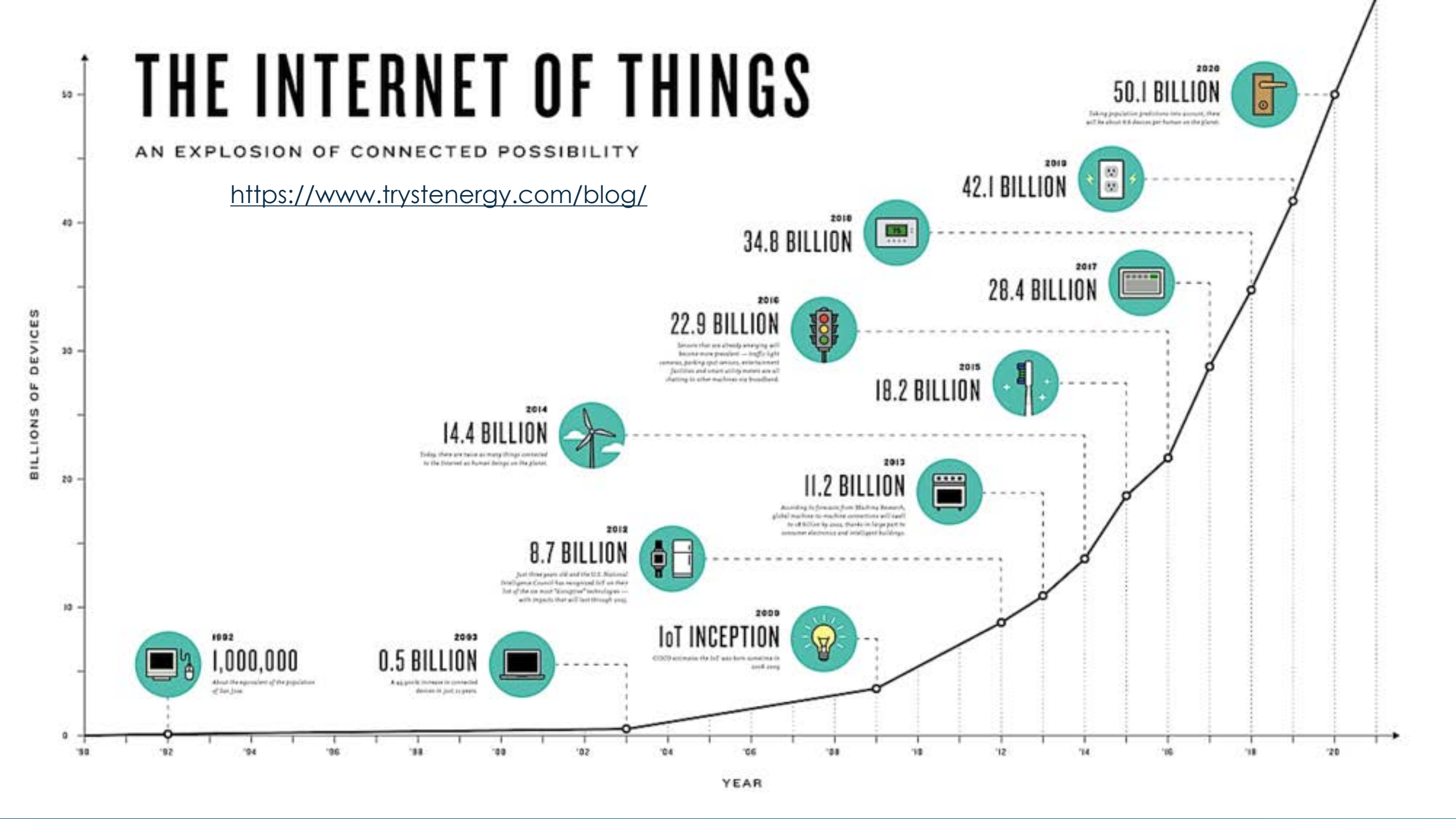
Network

Transportation

Retail

Industrial

Others


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
https://www.trystenergy.com/blog/
BILLIONS OF DEVICES
YEAR
1992
1,000,000
2003
0.5 BILLION
2009
IoT INCEPTION
2012
8.7 BILLION
2013
11.2 BILLION
2014
14.4 BILLION
2015
18.2 BILLION
2016
22.9 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION

Product Security

Great opportunities, but are our IT staff ready to secure products, IoT, ICS, OT?

2020

4 BILLION
Connected People

$4 TRILLION
Revenue Opportunity

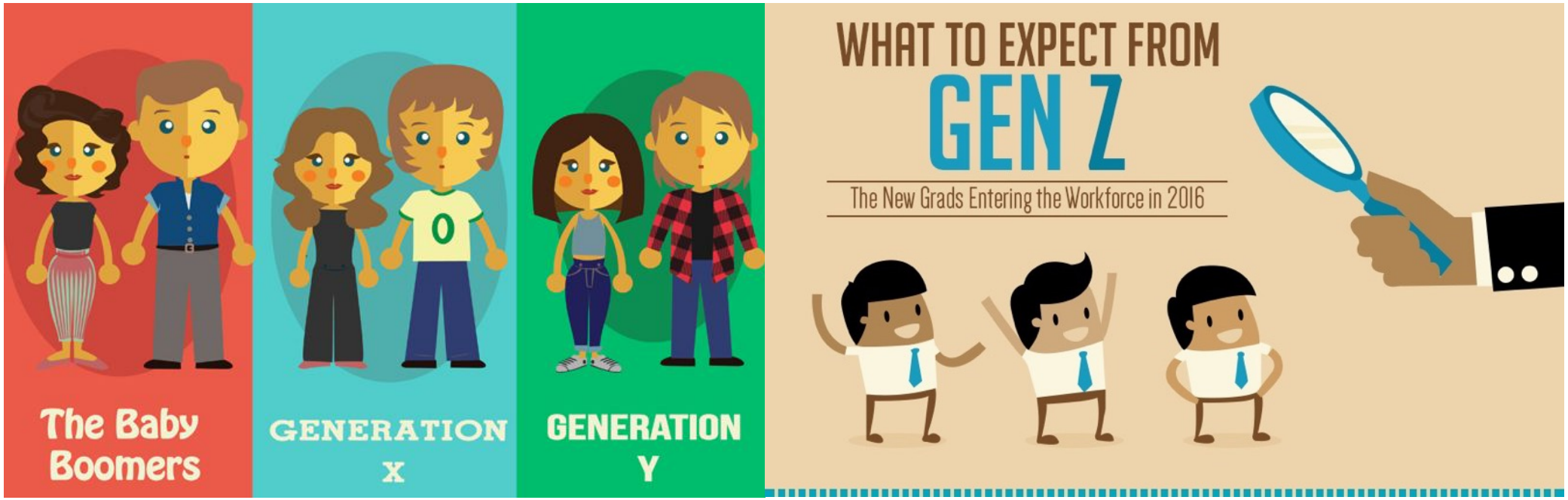
25+ MILLION
Apps

25+ BILLION
Embedded and Intelligent Systems

50 TRILLION
GBs of Data

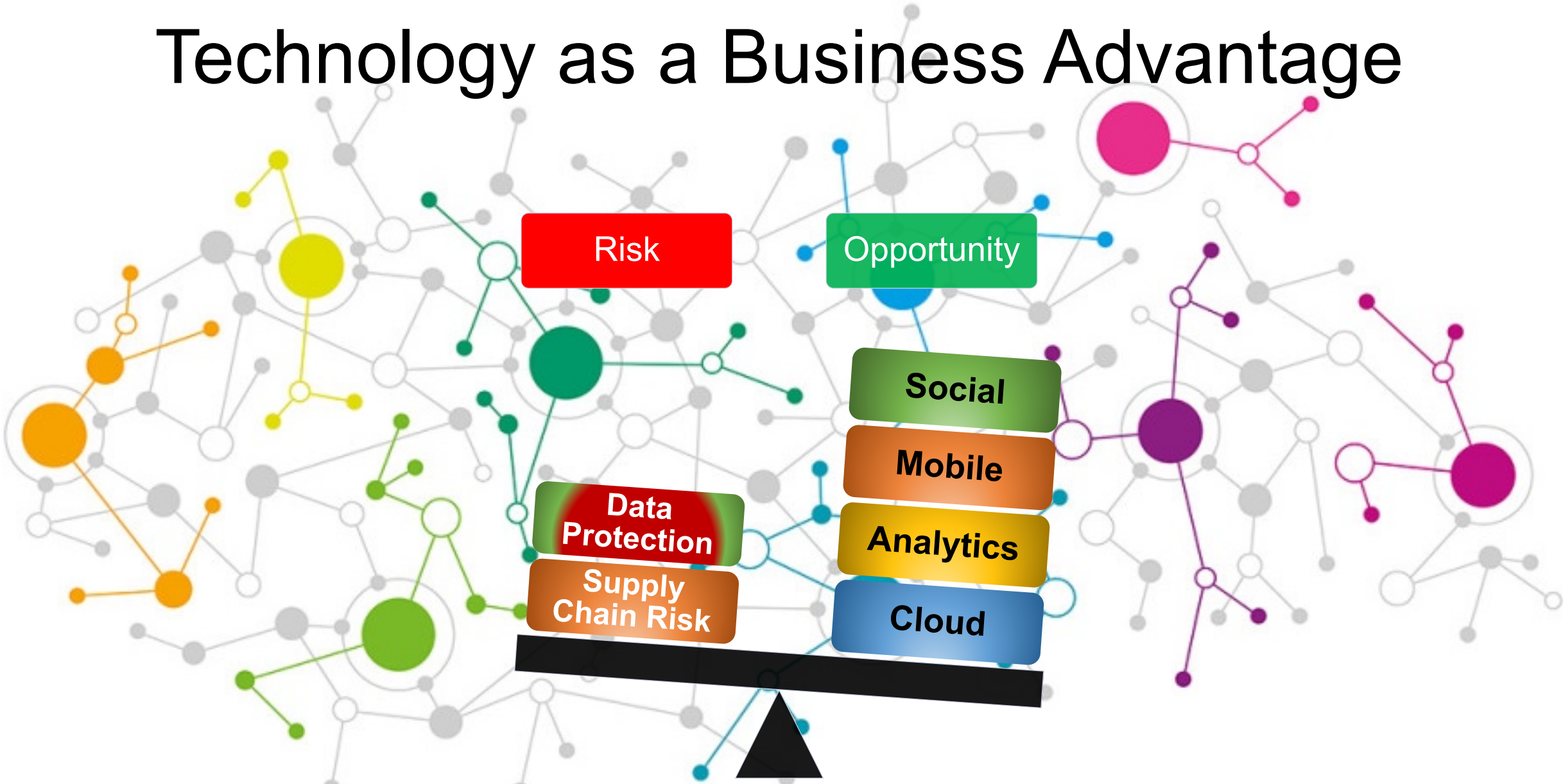
Source: Mario Morales, IDC

Different Stakeholders Want to Use Technology Differently



- Different Employee Segments
- Business Partners
- Customers
- Dealers / Resellers
- Business Leaders

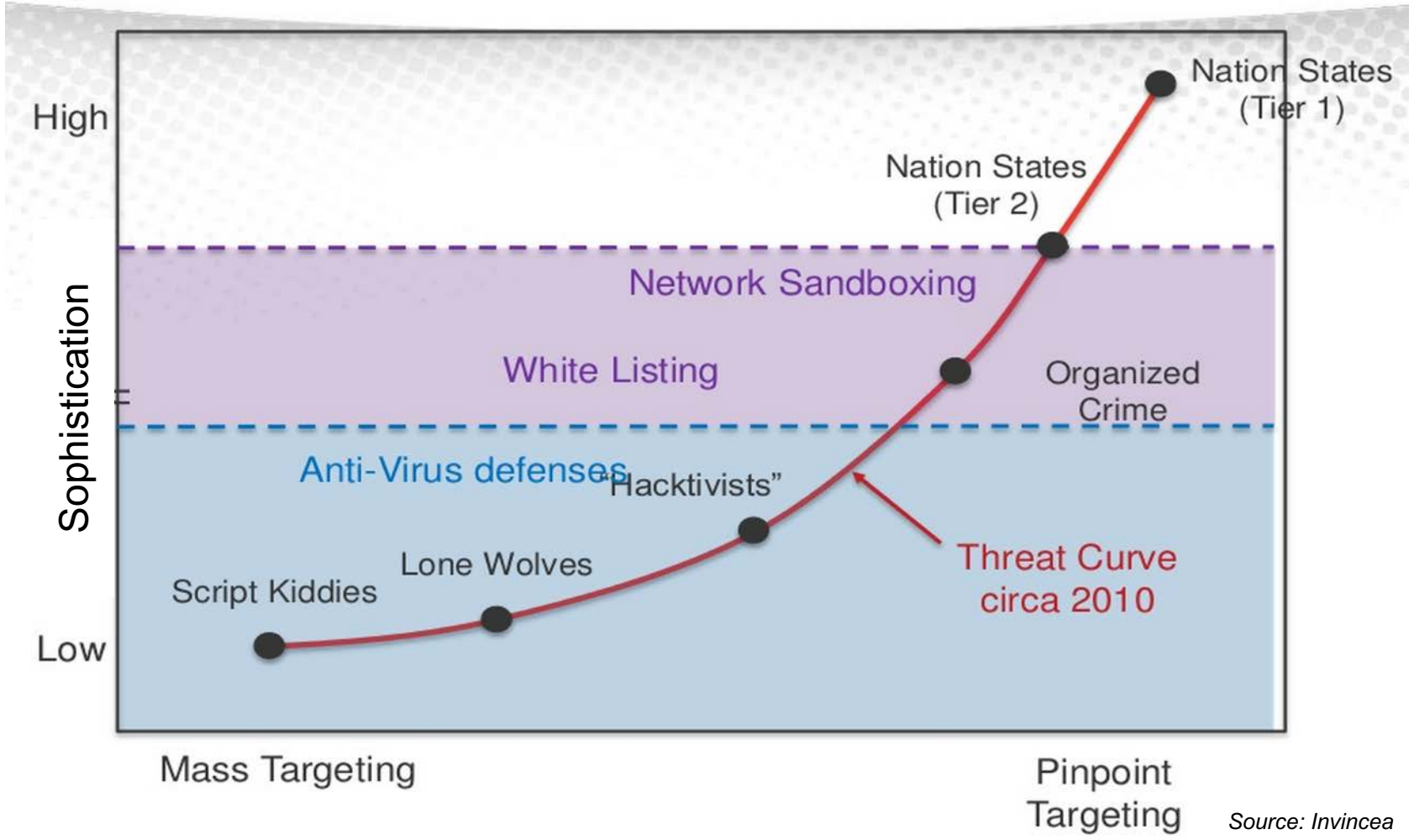
Technology as a Business Advantage



Today, technology makes a castle defense ineffective

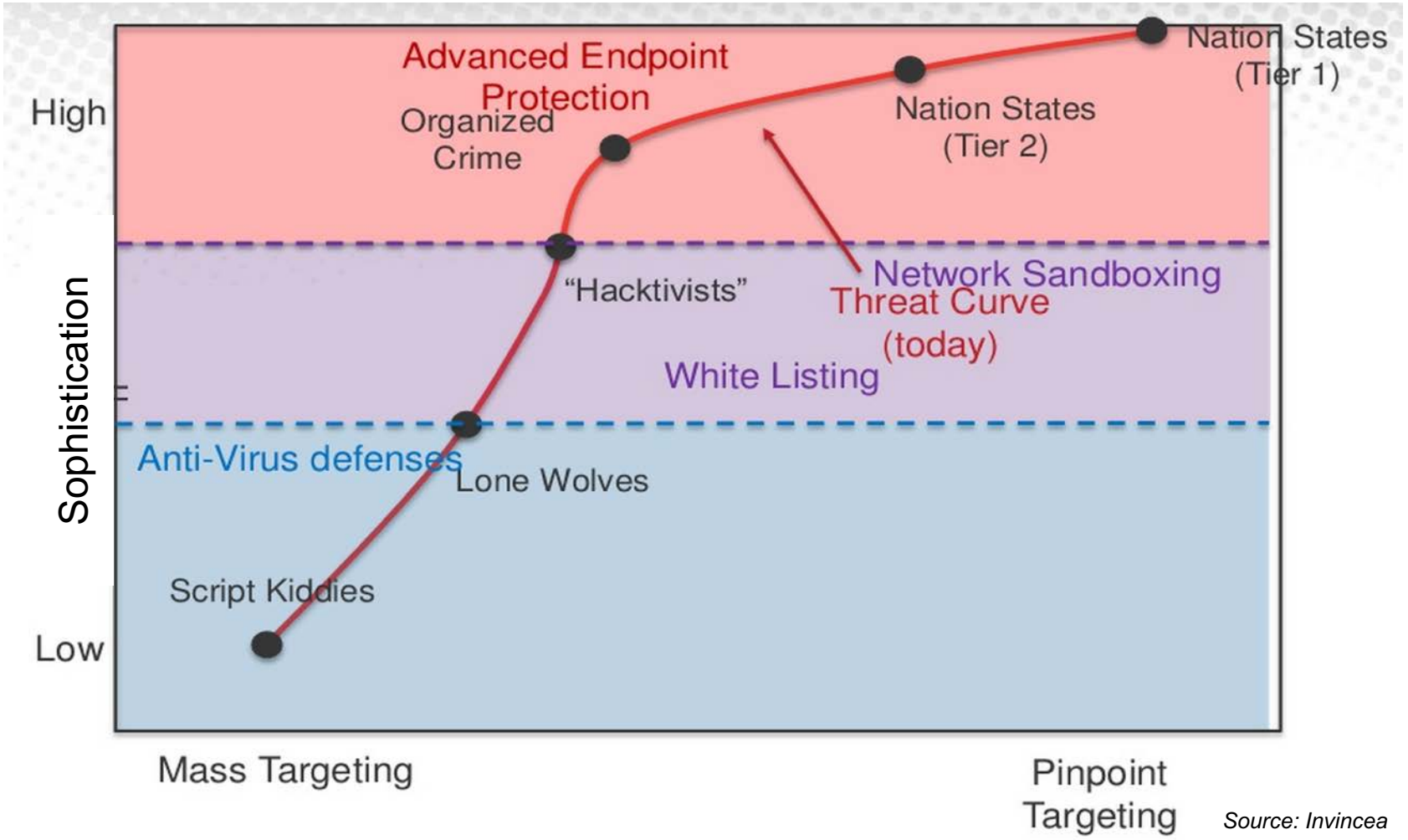
The Threat Landscape

Threat Capabilities - ***2010***



Source: Invincea

Threat Capabilities - ***Today***



Source: Invincea

Don’t Let This Happen To You

Data Breach Update & Highlights

October 3, 2017

Number of Breaches on pace to now hit 1,400 in 2017

As of October 3, the total number of breaches captured in the 2017 ITRC Breach Report now totals 1,056, an increase of 23.2 percent over last year's record pace for the same time period (857).

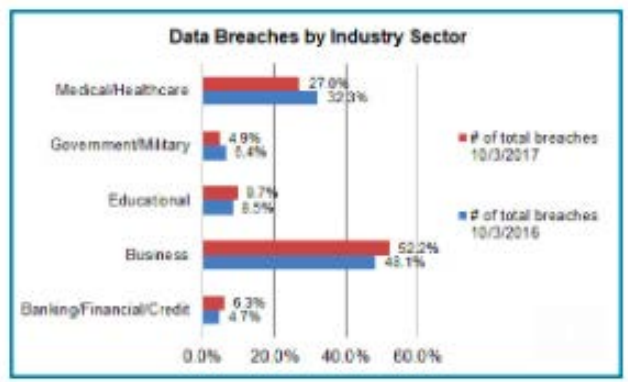
From 2005 through 10/3/2017, the ITRC has identified 7,956 data breach incidents.

	# of total breaches 10/3/2016	# of total breaches 10/3/2017	Percent Change (+/-) 2017/2016
Business	412	551	+ 33.7
Educational	73	102	+ 39.7
Government/Military	55	52	- 5.5
Medical/Healthcare	277	285	+ 2.9
Banking/Financial/Credit	40	66	+ 65.0
TOTAL	857	1056	+ 23.2

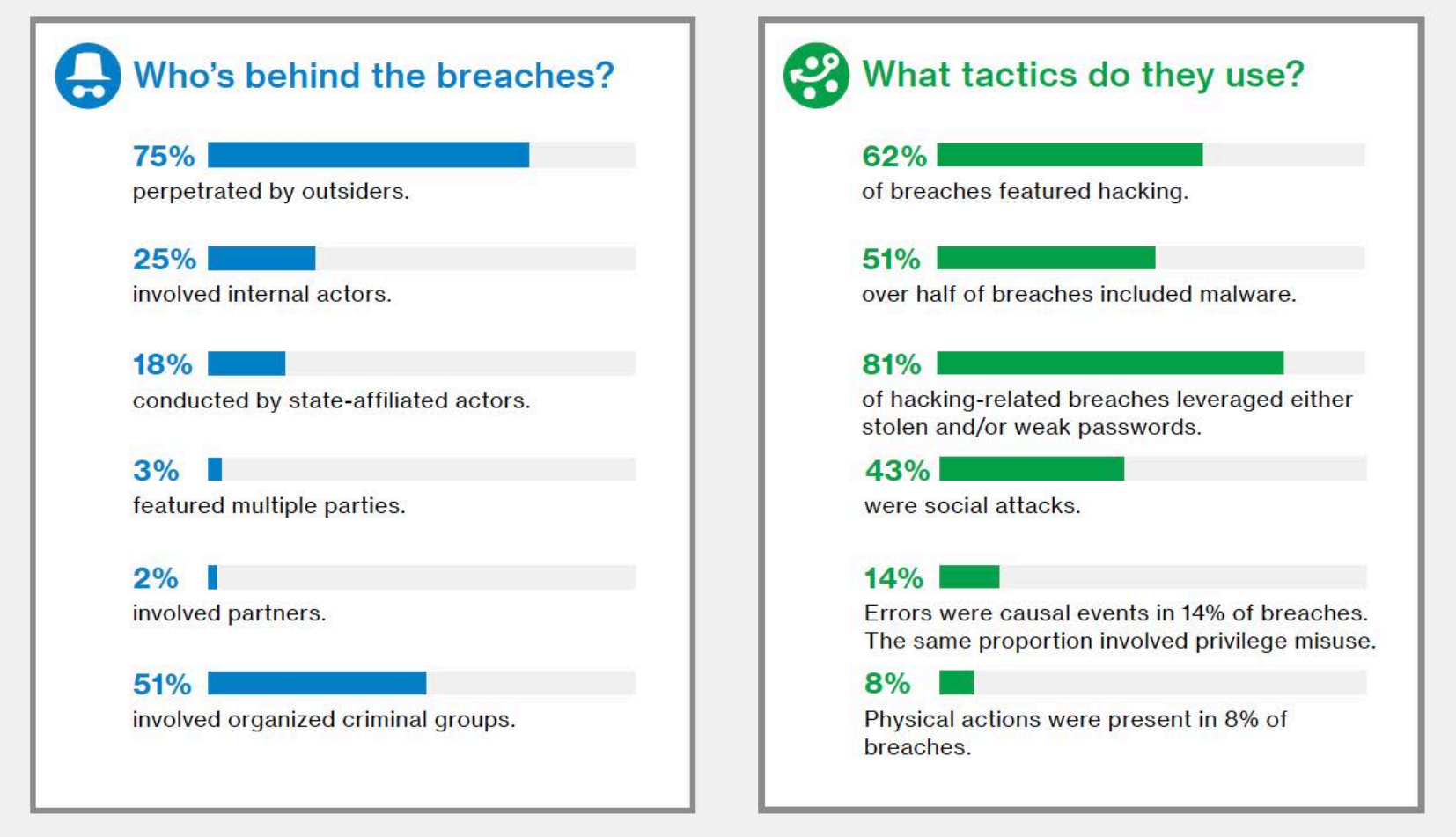
2017 Data Breaches

With 34 breaches recently added to the ITRC Breach Stats Report, the five industry sectors break down as follows (ITRC Data Breach Category Summary):

- Business = 52.2 percent
- Medical/Healthcare= 27.0 percent
- Educational = 9.7 percent
- Banking/Credit/Financial = 6.3 percent
- Government = 4.9 percent



Threat Actors



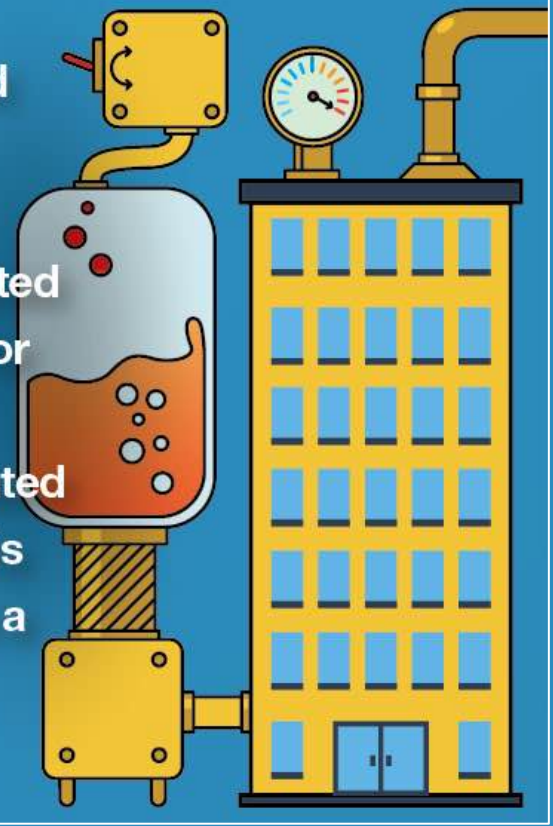
Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

20 BILLION IOT DEVICES ARE THE WEAKEST LINK FOR ATTACKING THE CLOUD

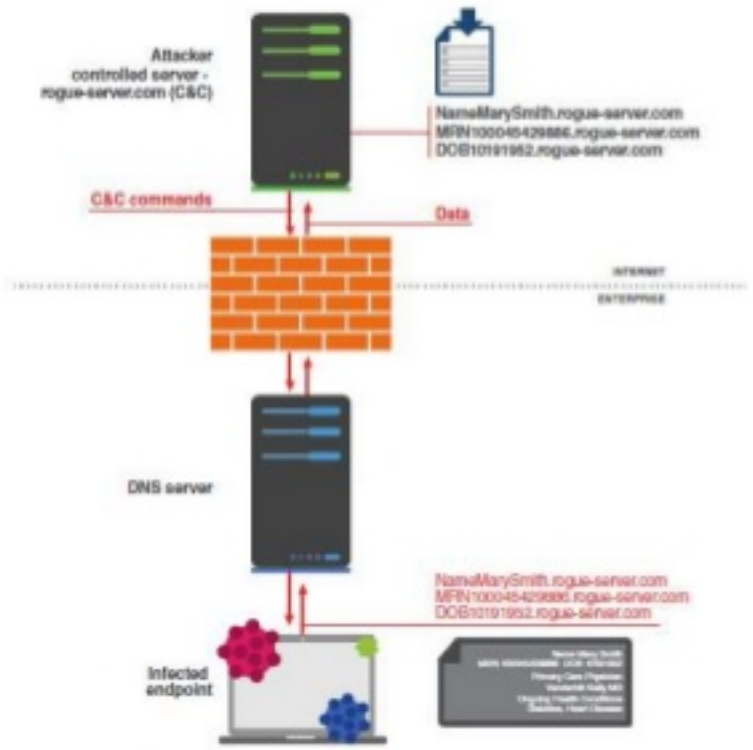
The weakest link in cloud security is not in its architecture. It lies in the millions of remote devices accessing cloud resources. We expect to see attacks designed to exploit endpoint devices, resulting in client side attacks that can effectively target and breach cloud providers.

ATTACKERS WILL BEGIN TO TURN UP THE HEAT IN SMART CITIES

As building automation and management systems continue to grow over the next year they will be targeted by hackers. The potential for massive civil disruption should any of these integrated systems be compromised is severe, and are likely to be a high-value target for cybercriminals.



“New” Threat Mechanisms — DNS Tunneling



Source: Infoblox

Source: Fortinet

The only things certain in life are death, taxes & GDPR

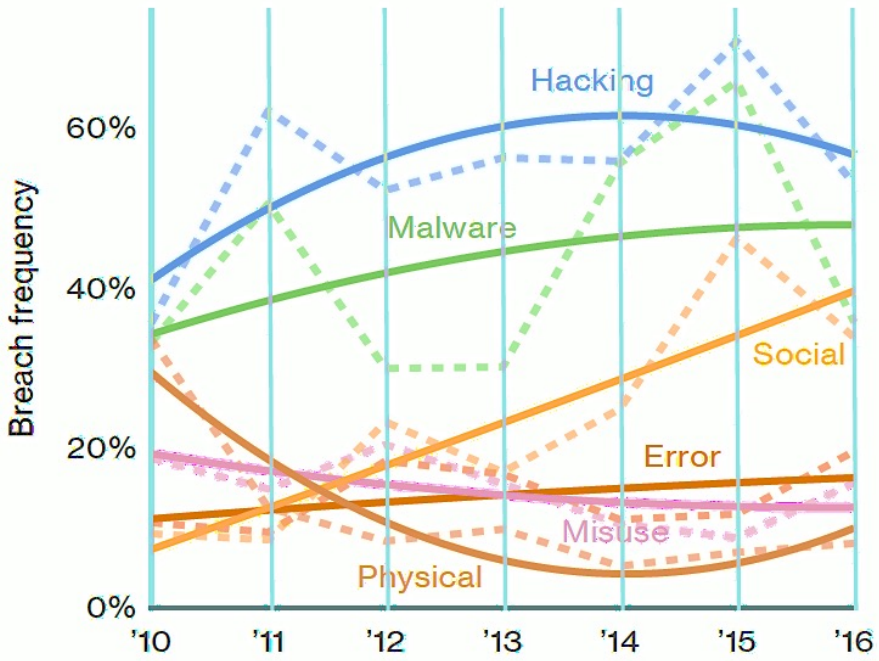
ISMS.online
Revolutionising information security management

Top Global Risks for 2017

Risk	2017 Rating	2016 Rating
Economic Conditions	6.61	5.83
Regulatory Changes and Scrutiny	6.51	6.06
Cyberthreats	5.91	5.80
Speed of Disruptive Innovation	5.88	5.48
Privacy or Identity Management & Information Security	5.87	5.55
Succession Challenges, Ability to Attract and Retain Talent	5.76	5.63
Global Market and Currency Volatility	5.67	5.33
Organizational Culture Hindering Escalation of Risk Issues	5.66	5.30
Resistance to Change Operations	5.63	5.40
Sustaining Customer Loyalty and Retention	5.62	5.28

Source: http://www.journalofaccountancy.com/news/2016/dec/top-business-risks-for-2017-201615723.html

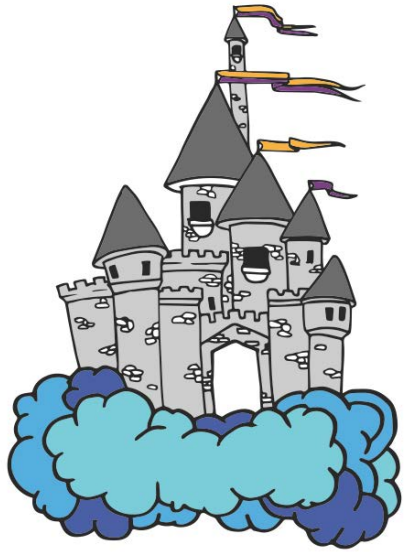
The Situation Today



The Volume and Sophistication and Automation of Attacks is Rapidly Increasing

We cannot enable business transformation if we are still trying to defend a castle. We need to mature our capabilities and strive for cyber resiliency.

Global Regulatory Changes



Data & Services Are Moving to The Cloud

Variety and Use of Technology

Building Resiliency

First: Overcoming Confirmation Bias

We must get over confirmation bias that tells us:

- We are doing a thorough job*
- We are doing a good job*
- We are adequately prepared for the future*
- Yesterday's technology, processes and thinking will solve tomorrow's problems
- We only need to be better than our competitors to avoid being compromised

* Most companies aren't. If you think you are, what is your evidence?

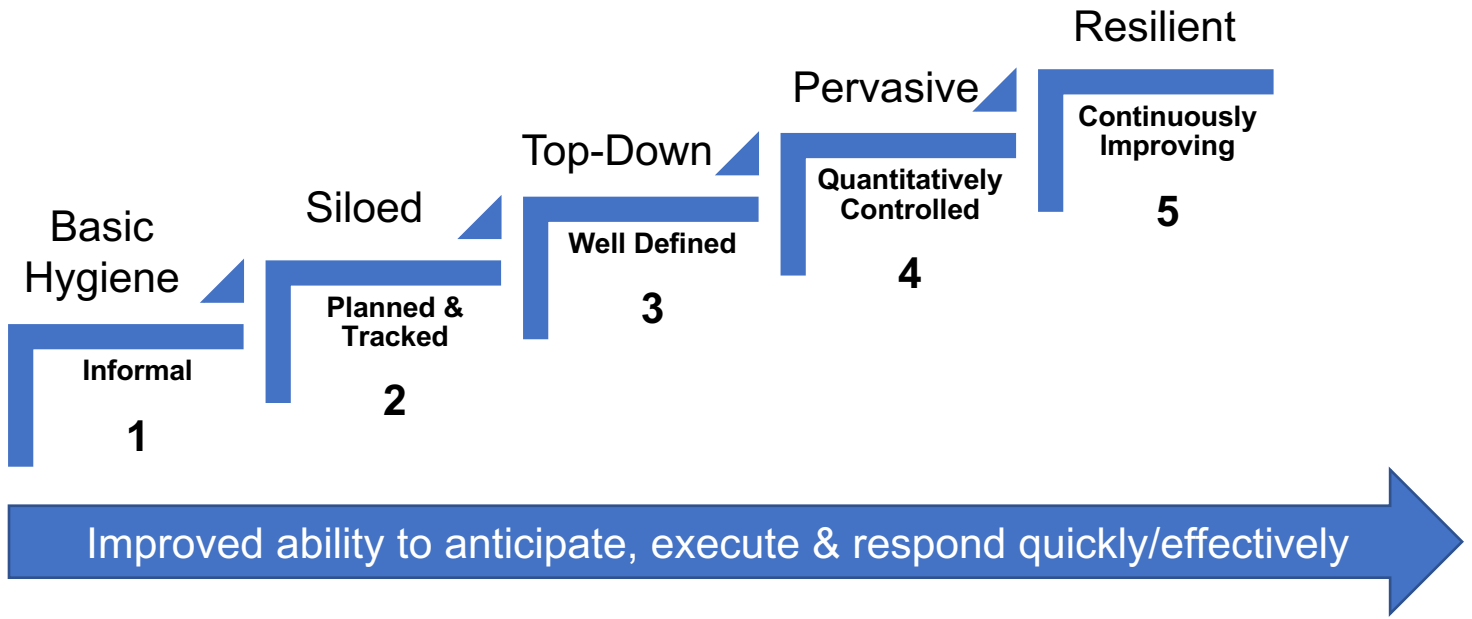

Our Adversary Is Not A Bear…
The Internet is Full of Bears.

#1 Capability Maturity

- Basic Hygiene – CIS Top 20
- Anchor to Standard Frameworks, Standards & Configurations
- Gain Situational Awareness

Capability Maturity

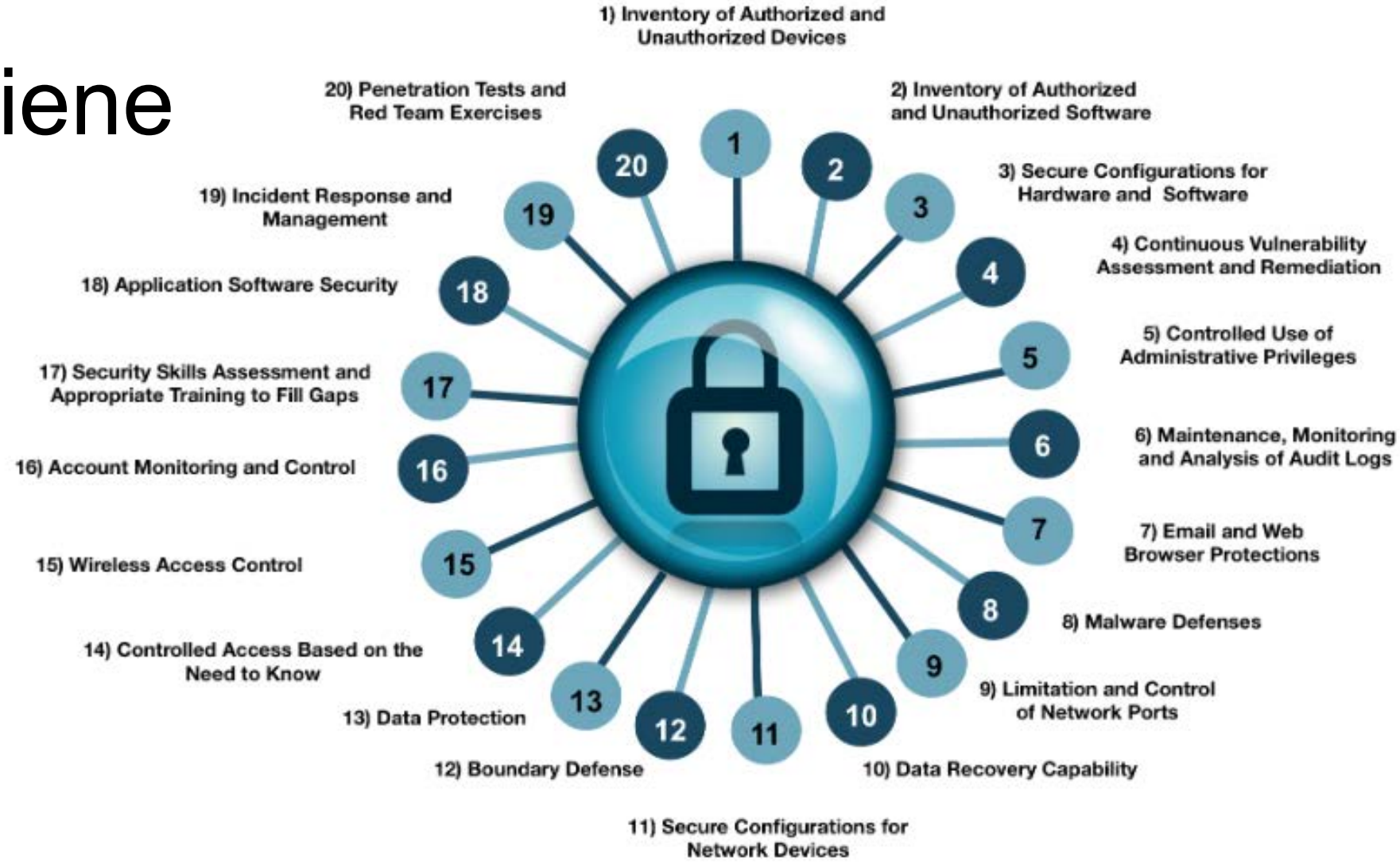
As the security program matures, more fundamental pieces will be in place to support advanced toolsets and capabilities necessary to protect against more advanced threats, respond faster to attacks and recover. The pace of threats, regulatory change and advancing technology require maturity and resiliency.



N.B. – Ponemon Self-Assessment ranges from -2 to +2

Business context will determine where you focus

Basic Hygiene



We start with ”Basic Hygiene”, such as CIS Top 20 Critical Security Controls.

Source: https://learn.cisecurity.org/20-controls-download

Anchor Cybersecurity Program Using Standard Frameworks

* NIST Cybersecurity Framework

Baseline Configurations

CIS also has baseline security configurations for systems and software. This allows you to set a security baseline (with documented variances) which maps back to a framework (NIST CSF) – good security based on industry standards which you can audit against using automation.

- OS Platforms: Linux, Novell, Unix, MS Windows, Apple Mac OS
- Amazon AWS (Hardened virtual images in EC2)
- Browsers: Chrome, Firefox, MS IE, Opera, Safari
- Microsoft Office, SharePoint, MS Exchange, Apache, IIS
- Mobile Device Platform OS: Apple iOS, Android
- Network Devices: Cisco Devices, Juniper, Palo Alto, CheckPoint, Wireless Network Devices
- Multifunction Printers
- Databases: IBM DB2, MS SQL, Oracle MySQL, Oracle DB, Sybase
- Virtualization: Docker, VMware, Citrix Xen

If you know the enemy and know yourself you need not fear the results of a hundred battles.

Sun Tzu

Situational Awareness – Understanding the Current Posture and Threats

- Can’t assess risk without knowledge; turn uncertainty into a risk measurement (risk-based security management)
- **Know the Enterprise**:
  - Identify your Assets: Enpoints, Data, Applications, Network, Identities…
    - What is their function? Where are they? What is their posture?
  - What is your exposure? Where are you vulnerable?
- **Know the Business**: What is important, learn business processes
- **Know the Enemy**: A case for actionable Threat Intelligence & Information Sharing
- Root Cause Analysis and Attribution can tell you where to focus (access to historical and forensic data)

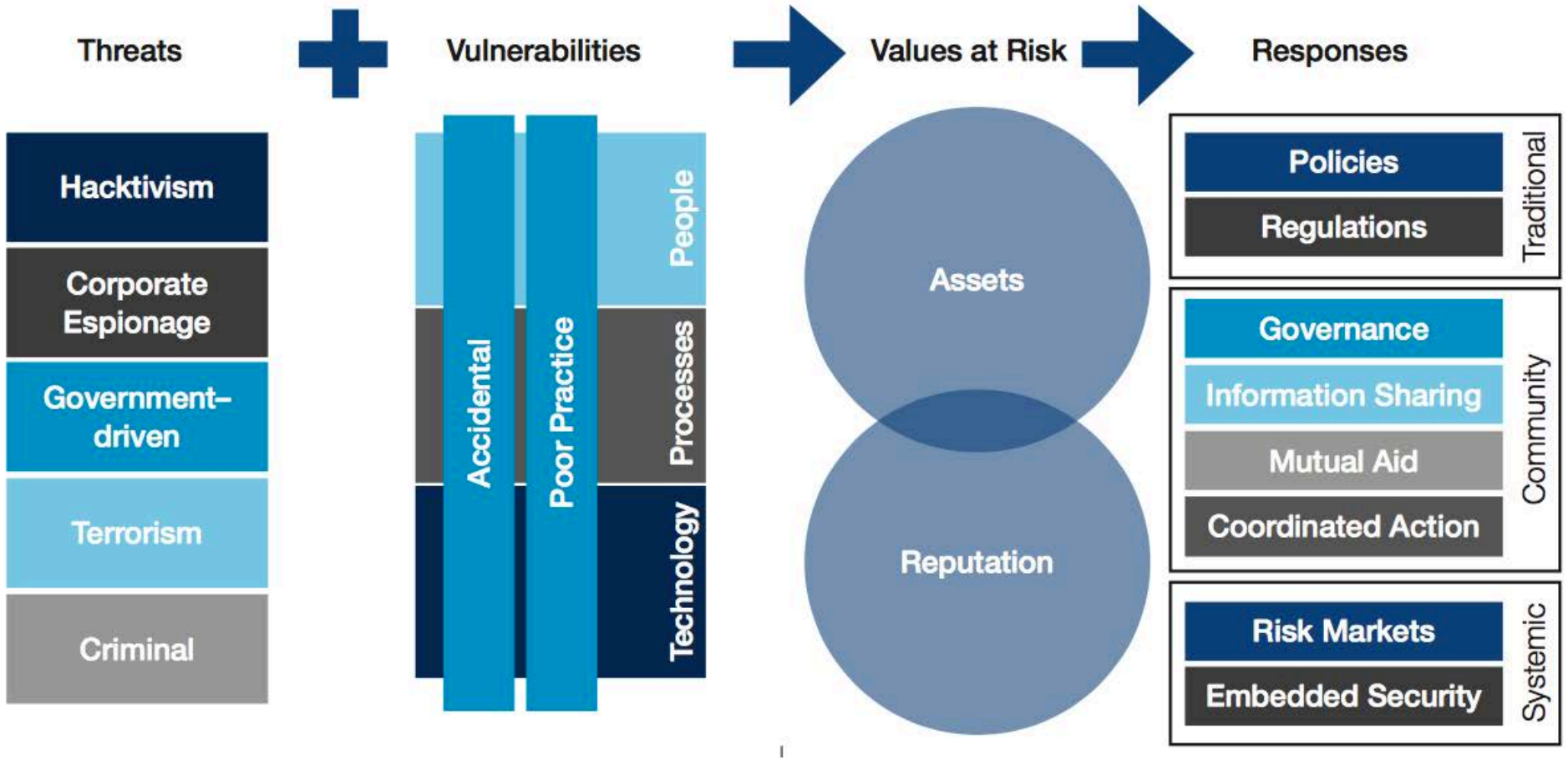
Asset Vulnerabilities and Value

- Knowledge of posture gives vulnerability, and along with understanding threats and value of resources, risk can be calculated
- Look for solutions that help you aggregate information from disparate sources about assets (much different from SIEM):
  - System configuration, patch levels and OS details
  - Details about desktops, servers, cloud-hosted, BYOD, non-compliant systems, OT systems and ICS
  - Inventory of software and versions installed
  - This is not the same as vulnerability scanning
- Centralizing this information is key – avoid delays from running to various IT teams whenever you need to gather compliance/IR details

#2 Focus on Value at Risk

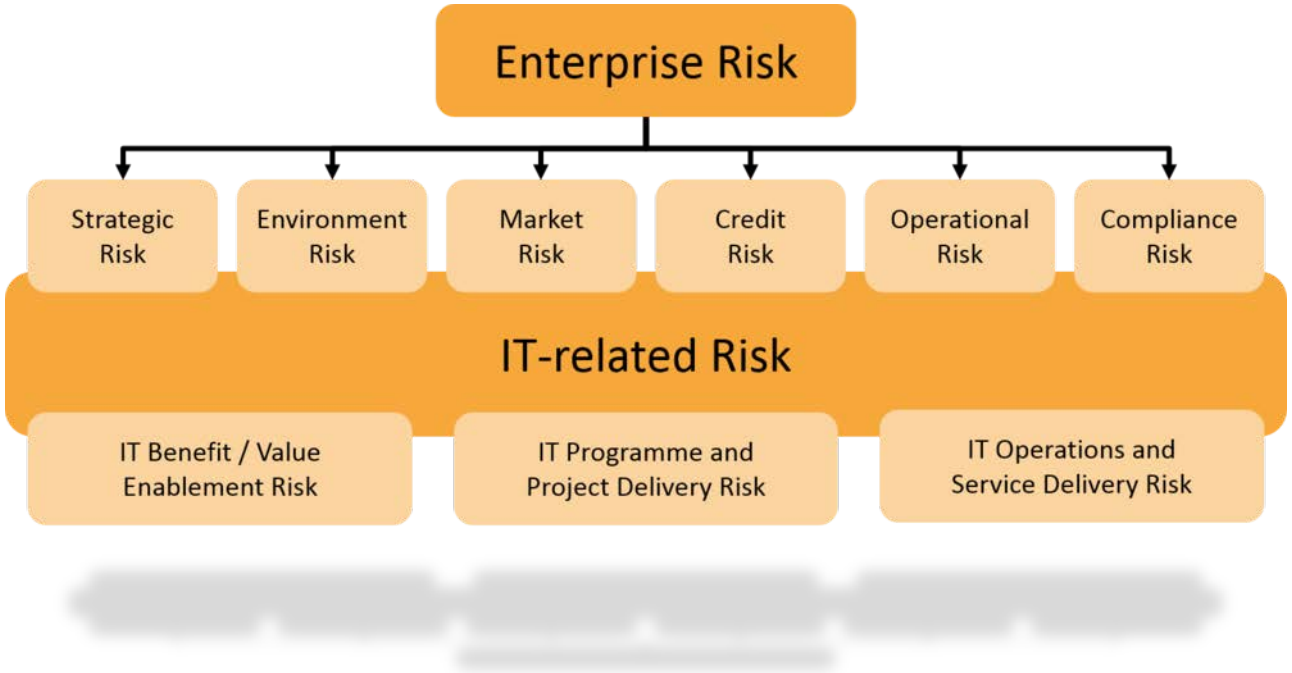
- Adopt a Risk Management Framework, Aligned w/Enterprise Risk
- Assess Current State in Context of Business
- Model Threats & Consequences
- Apply Layers of Controls
- Utilize Metrics to Measure Efficacy of Controls
- Training & Awareness
- Prepare & Practice

A Cyber Risk Framework Improves Resiliency



Source: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

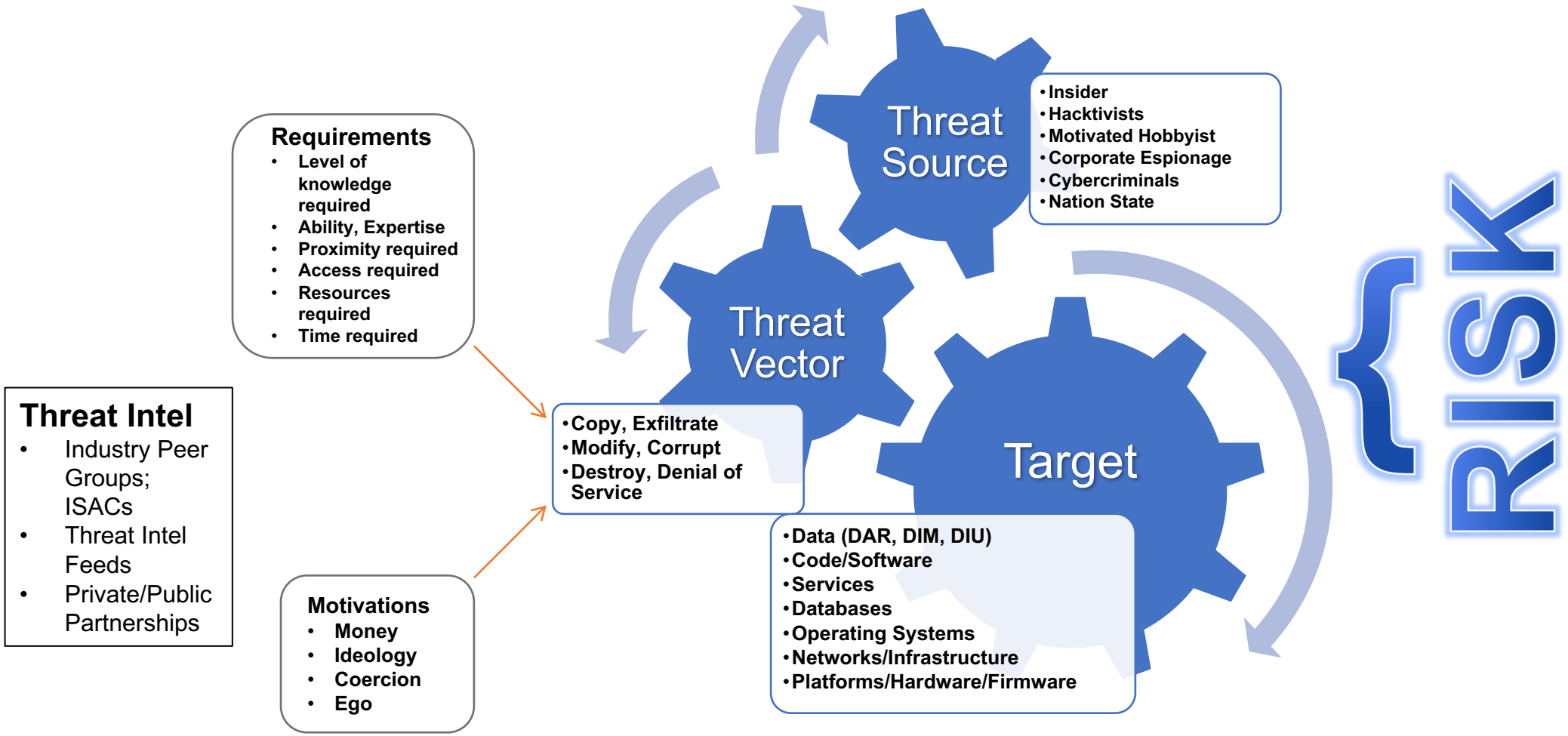
IT Risk in the Risk Hierarchy



Understand how IT Security Risk cuts across all aspects of Enterprise Risk

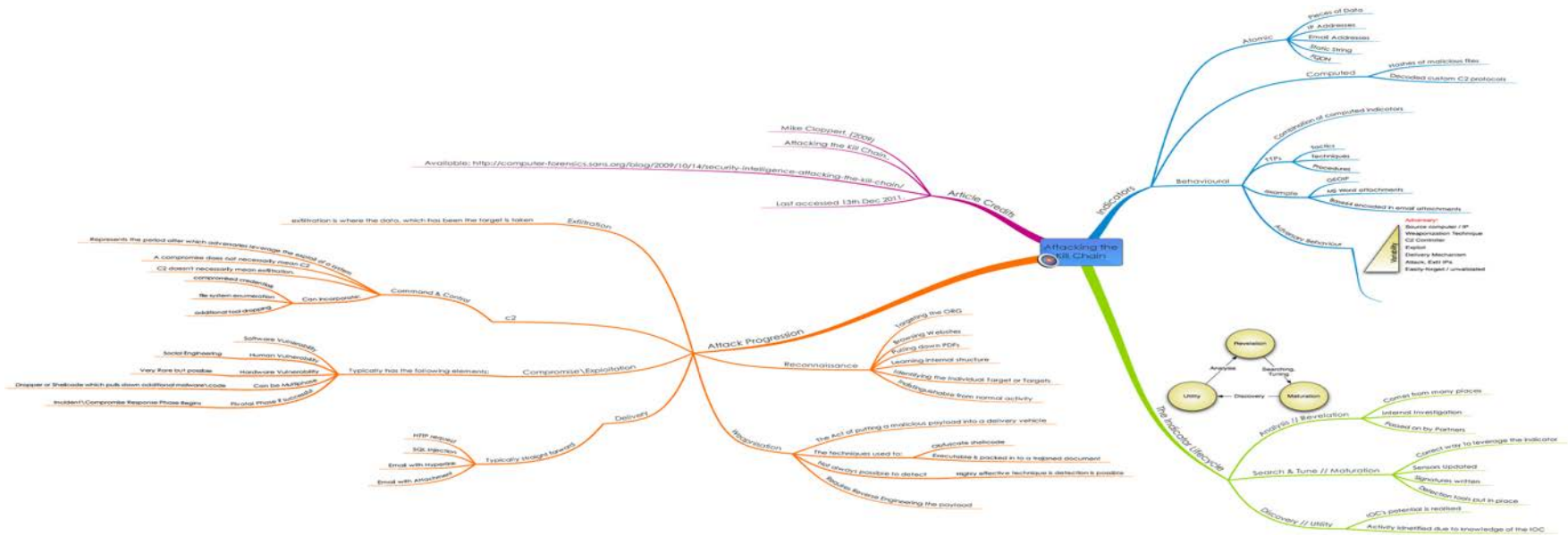
Source: COBIT

Cyber Risk Analysis: Threat Modeling

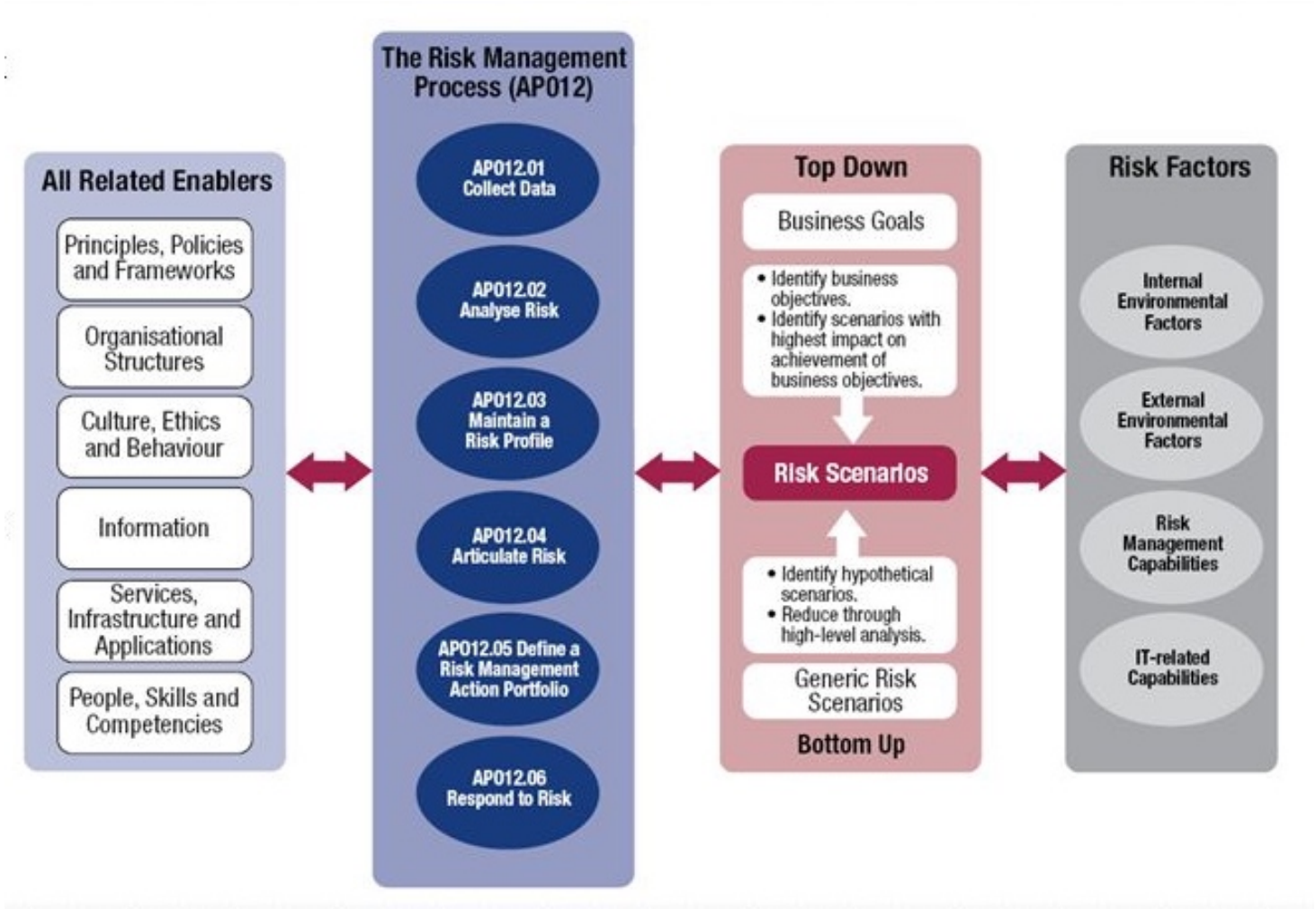


Risk can be mitigated; the threat landscape remains unchanged.

Attack Chain Mapping and Threat Modeling

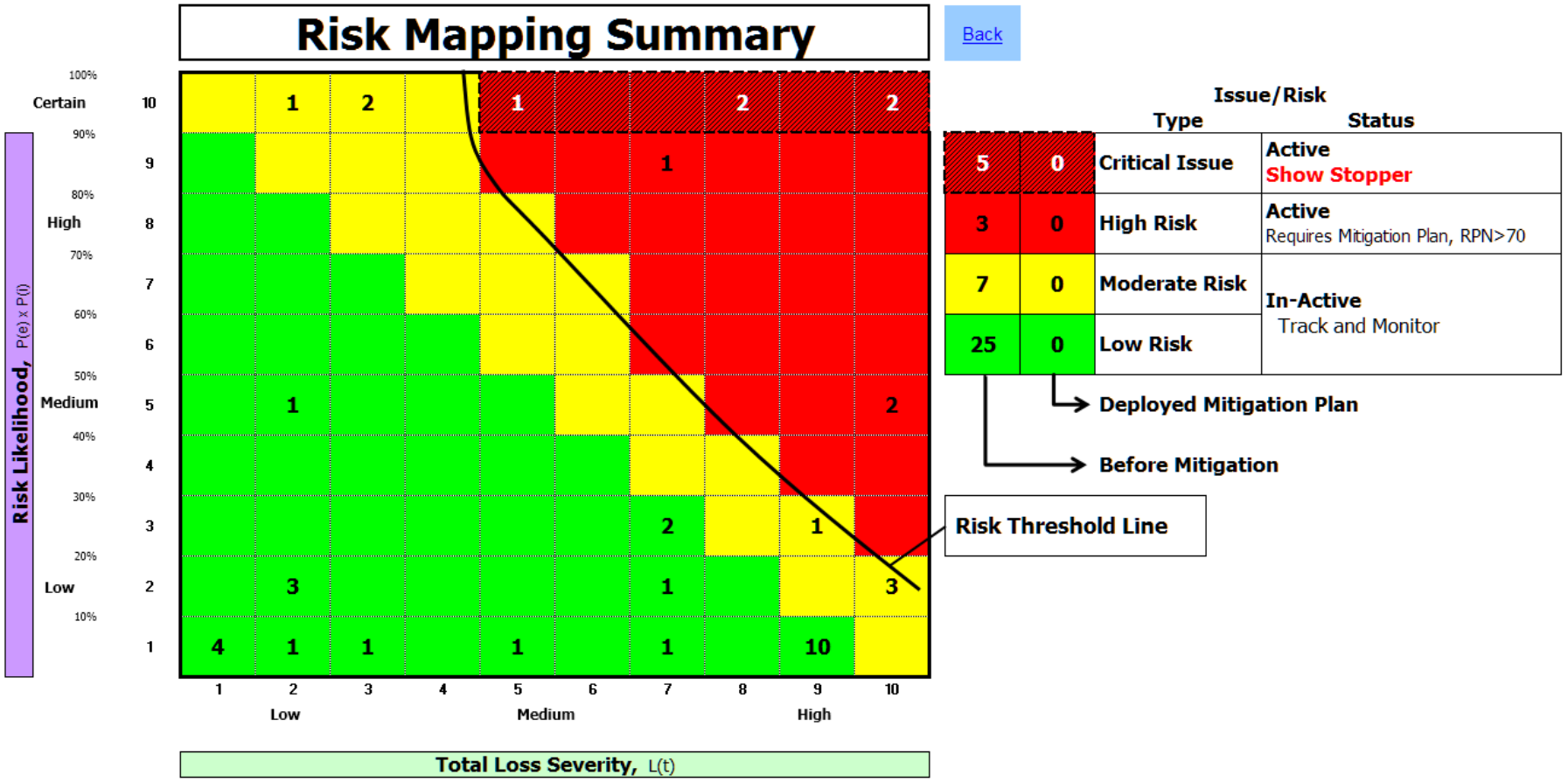


Risk Scenario Overview



Source: COBIT

Risk Analysis (Example)



Respond with Layers of Controls

Once we have assessed our security risk we identify controls to mitigate risk, or we transfer or accept risk. [Risk transfer includes cyber insurance.] Controls may be technical, but also involve people and processes. They may be "traditional" or leverage new technology, such as machine learning.

SECURITY SYNERGY

To determine the total effectiveness of one or more synergistic controls, use the following equation (E = effectiveness of a single control). As the chart indicates, using multiple ineffective controls together results in effective control overall.

Baye's Theorem: $E_{total} = 1-((1-E1)*(1-E2)*(1-E3)...)$

# of Synergistic Controls	Efficacy of Each Control			
	60%	70%	80%	90%
1	60.0%	70.0%	80.0%	90.0%
2	84.0%	91.0%	96.0%	99.0%
3	93.6%	97.3%	99.2%	99.9%
4	94.7%	99.2%	99.8%	100.0%
5	99.0%	99.8%	100.0%	100.0%

Risk can never be eliminated, but it can be mitigated. Layered security is the most effective way to do this.

Metrics Measure Effectiveness of Controls

So why do we want security metrics?

Ask:

- Are we being effective?
  - Performance
  - Controls/Processes
  - Risk Management
- Are we efficient?
- Are we strategically aligned?
- Are we maturing our capabilities?
- Are we doing well compared to others?

Risk Based Security Management Roadmap

- Understand Current State
  - Environment (assets (value/inventory/vulns/compliance…), networks, data, applications)
  - Business knowledge (requirements, processes…)
  - Regulatory environment
  - Threats (std process for threat modeling/assessment)
  - Capability maturity
- Determine Risk
- Prioritize Security Portfolio
  - Business Alignment and Enablement
  - Reduce Risk (Business will choose to Accept, Transfer or Mitigate)
  - Build capabilities (maturity)
- Develop Metrics (operational → tactical → strategic)
  - Measure effectiveness of controls at risk reduction
  - Measure efficiency (are resources going where they add the most value?)
- Communicate Business Value

If everything is protected equally, nothing is protected adequately.

Training Security Staff

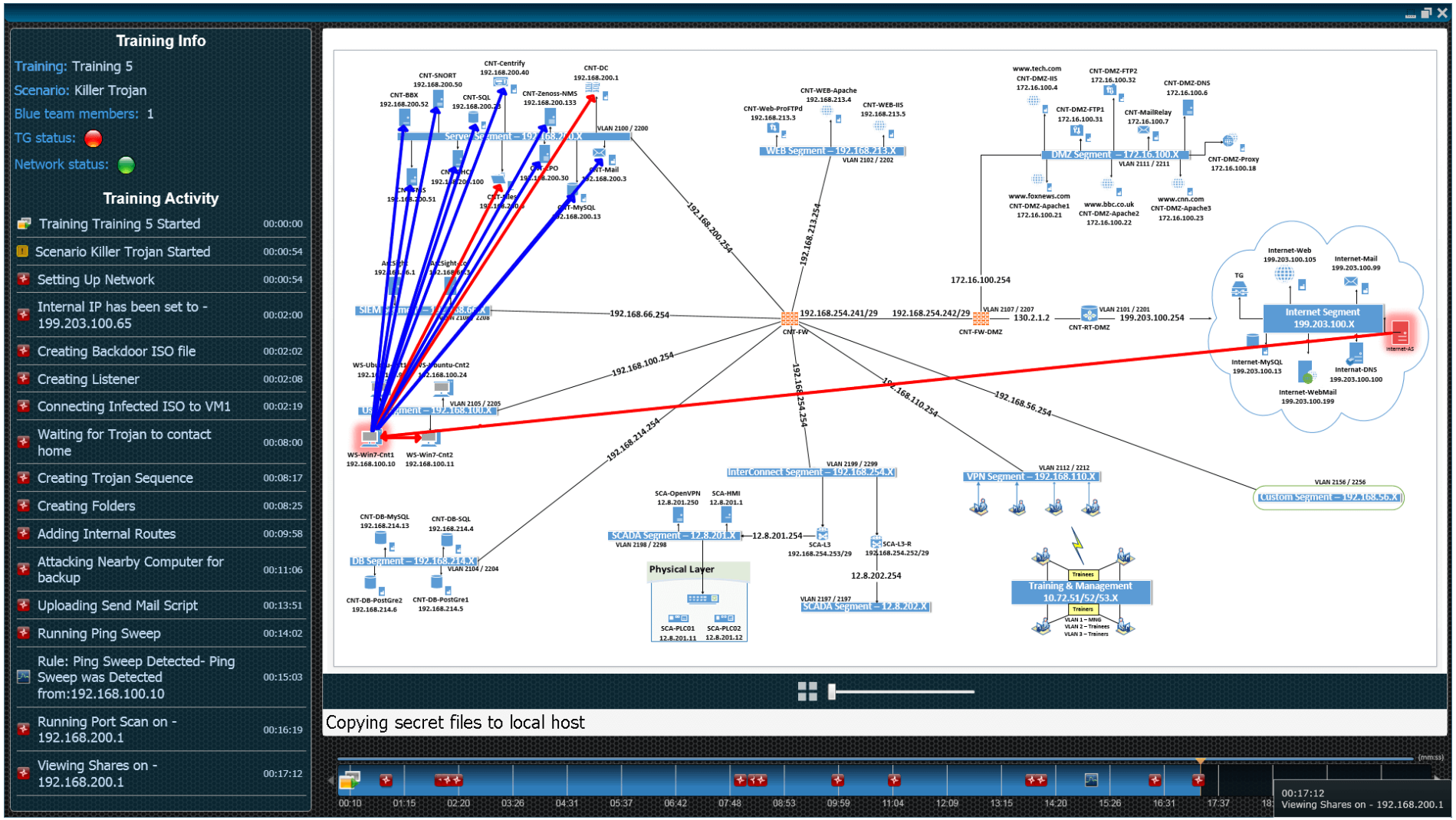
- Your security staff, and others in your organization (as you embed security across the organization) will need appropriate training.
- Example: Can your IT staff really apply IP network security techniques to secure IoT, OT, ICS?
- Training, mentoring and providing a career path is also key for attracting and retaining the best
- Smaller organizations may not be able to support the number of experts (or attract and retain) and should consider managed services

Key Aspects of a Successful Awareness Program

Security awareness should have:

- Executive sponsorship – *walk the walk*
- Targeted content and delivery methods depending on the audience
  - Classroom, CBT, Teachable Moments, Easy to find Policies & Procedures
- Clearly articulated goals
- Metrics to measure program efficacy and success
- Metrics and surveys to ensure program improvements
- Content that emphasizes in a meaningful way, why security is an important part of every employee's job
  - Understand the impact to the company and consequences of not following the rules
- Security solutions should be designed with the user experience in mind
  - If the secure way is the easiest way, people are less likely to choose Shadow IT

Perform Exercises and Practice



#3 Security Leadership

- Align Security Strategy with Enterprise Strategy
- Speak in the Language of the Business
- Lead by Example
- Build Relationships – *wear out your shoes*
- Communicate Effectively with Different Stakeholders
- Build a Culture of Security – *people believe the secure way is the better way*
- Break Down Siloes
- Consider Org Chart Changes

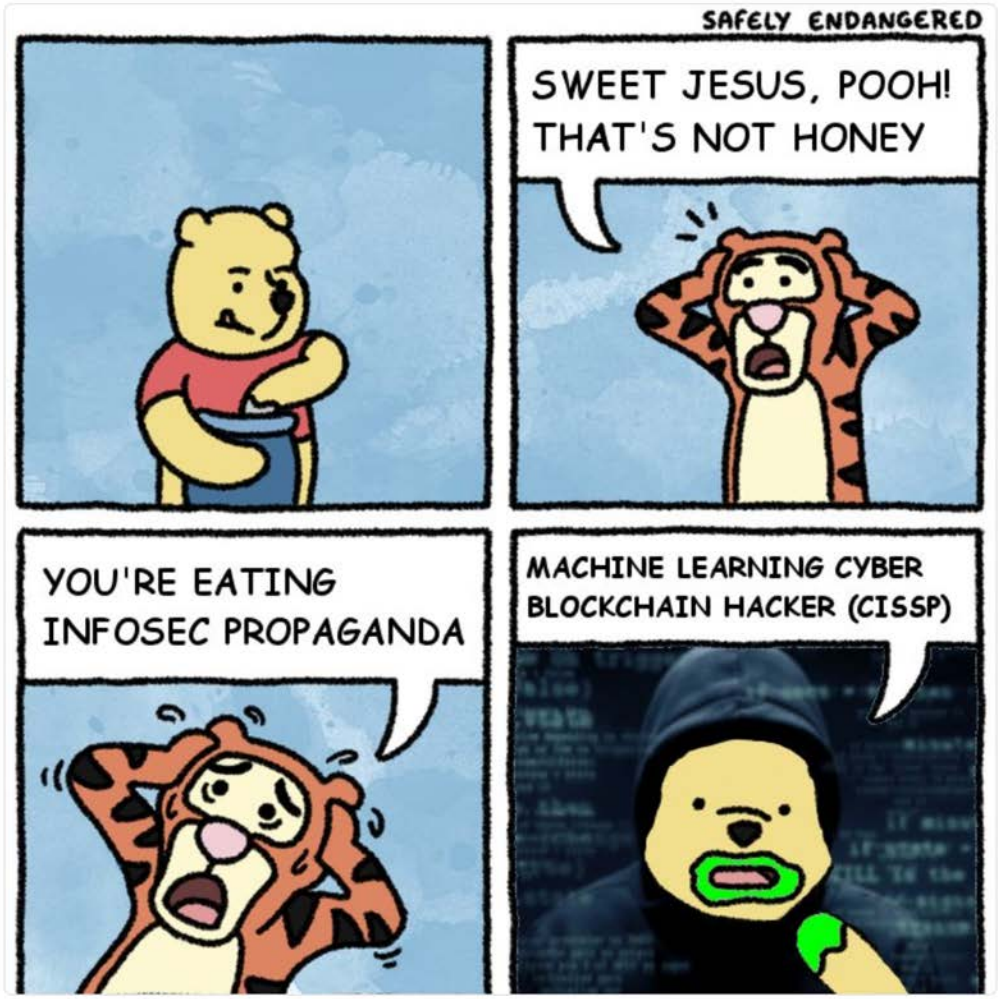
#4 Utilize Advanced Techniques & Technology

- Apply New Thinking to New Problems
- Utilize Automation for Greater Consistency and Speed
- Utilize New Technologies as Force Multipliers
- Innovate and Stay Ahead of the Curve

svbl
@svblxyz

Follow

🙃



4:01 AM - 3 Oct 2017

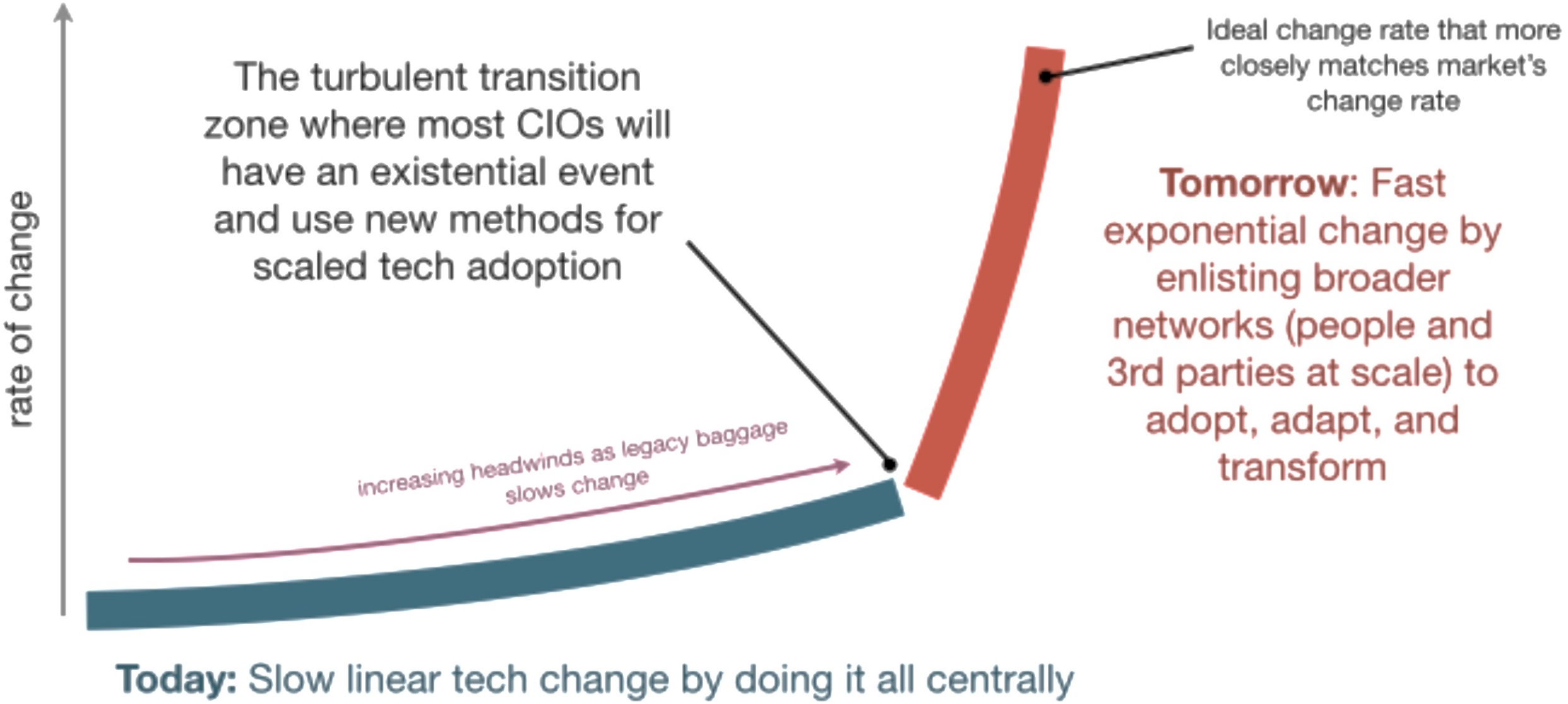
1,263 Retweets **2,249** Likes

13 1.3K 2.2K

05 OCT 17 NEWS

#Infosec2017: To Manage Risk Effectively, Unconventional Controls Are Needed

How Traditional IT is Untenable And Why New Models are Needed



By Dion Hinchcliffe, ZDNet

Future Tech

- 5G Communications
- Blockchain Proliferation
- Quantum Computing
- Fog: *push cloud computing to the edge (decentralize)*
- Mist: *push analytics & decision making to edge device*
- Rain: *computing is fully distributed, resilient and scalable, and integrated into the world around us*

These technologies are no longer in the distant future.
They hold great promise and benefits, but will be highly disruptive.
When they arrive, they will transform how we work and live.
We cannot secure them with an old mindset.

Source: ISACA

2017 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X **RATE OF CYBERSECURITY JOB GROWTH** VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

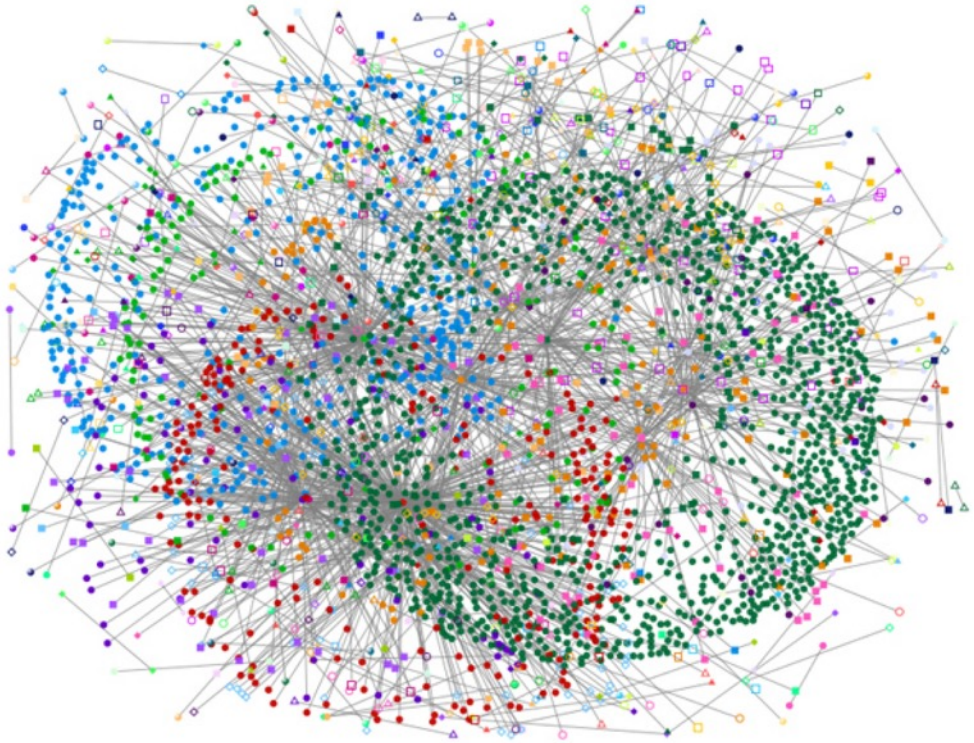
77% **OF WOMEN** SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% **OF U.S.** CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

New Tools for New Problems

- Key and Certificate Management at scale
- Cloud Security Access Brokers & Cloud Proxies
- Solutions to help give you situational awareness
- Improved Threat Intelligence (timely, detailed, actionable, integrable)
- Continuous Risk Profiling
  (if you have Posture, Value and Threat Info → RISK)
  - Near real-time view to quantitative and actionable enterprise risk
  - There are vendors today that will give you an overall risk score that you can compare to peers in your industry – not perfect but proven beneficial
- Automated Red Team Testing

AI and Machine Learning



High-risk, cross-data patterns existing tools cannot see

No amount of human analysts can solve for this systematically at scale

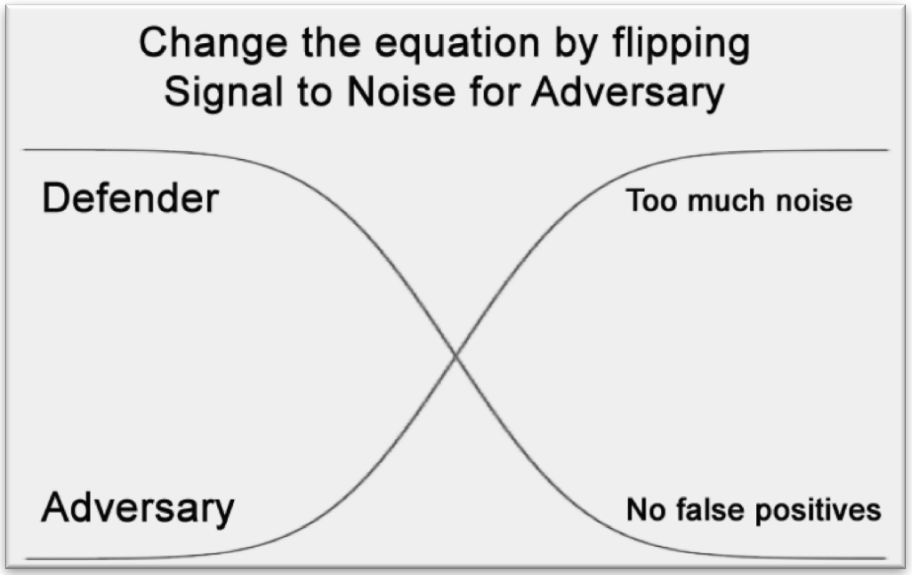
Source: Versive

AI and Machine Learning

- Our goal should be to detect and respond → Better and faster
- Today's SOC won't serve our needs in the future, need to rethink the approach – requires more and more analysts over time
- Tier I in the future will need to be AI, identifying patterns that are too fast or too slow or fly under the radar for humans with eyes that are tired of starting at a pane of glass → Put intelligence closer to the problem
- Identify/Correlate patterns across kill chain → Build Threat Cases
- Humans have an important role. AI can provide a faster view to situational intelligence and become a Force Multiplier letting the human focus on what humans are good at and be more effective

Fog of War – Deception Technology

- Raise the bar for the adversary – Reduce adversary's operating surface and increase their economic cost
- By adding lots of noise for adversaries it becomes hard to avoid false leads which give them away.

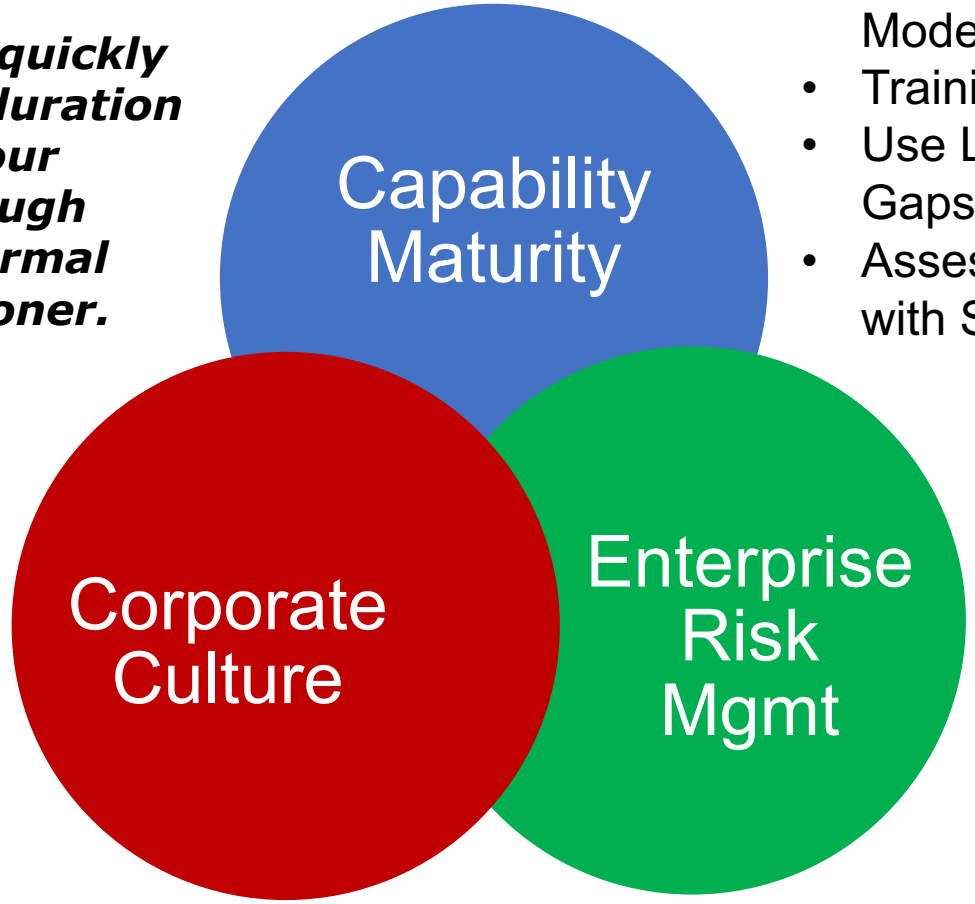


Cyber Resilience

BETTER • FASTER • PREPARED

Goal: Prevent or respond quickly to reduce the impact and duration of threat events to your organization, and through preparation, restore normal business operations sooner.

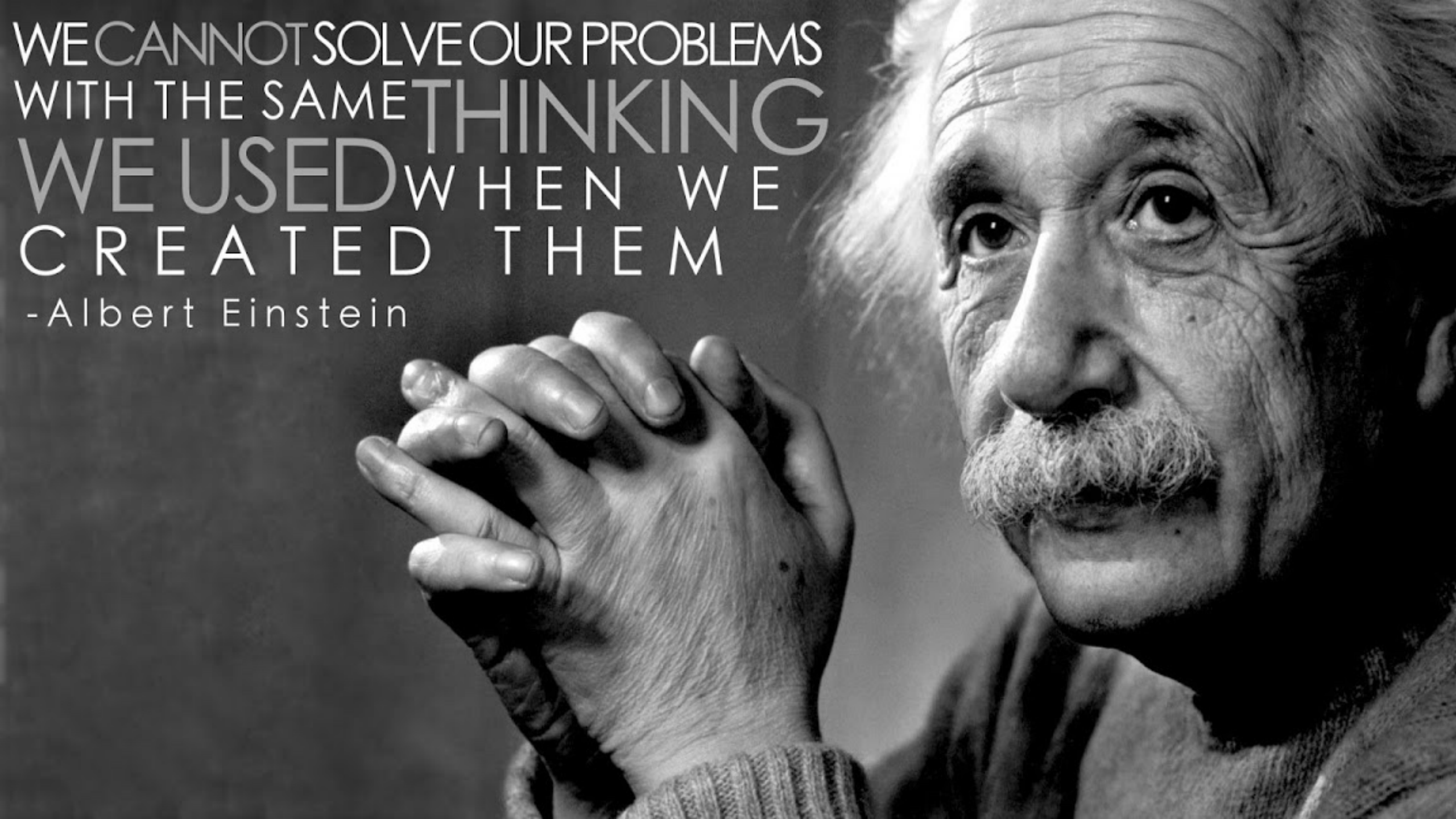
- Basic Hygiene
- Anchor to Standards Frameworks
- Baselines & Compliance
- Risk Based Security Management
- Threat Intelligence, Assessment & Modeling
- Training and Practice
- Use Layered Security to Address Gaps – People/Process/Tools
- Assess Effectiveness of Controls with SMART & Meaningful Metrics



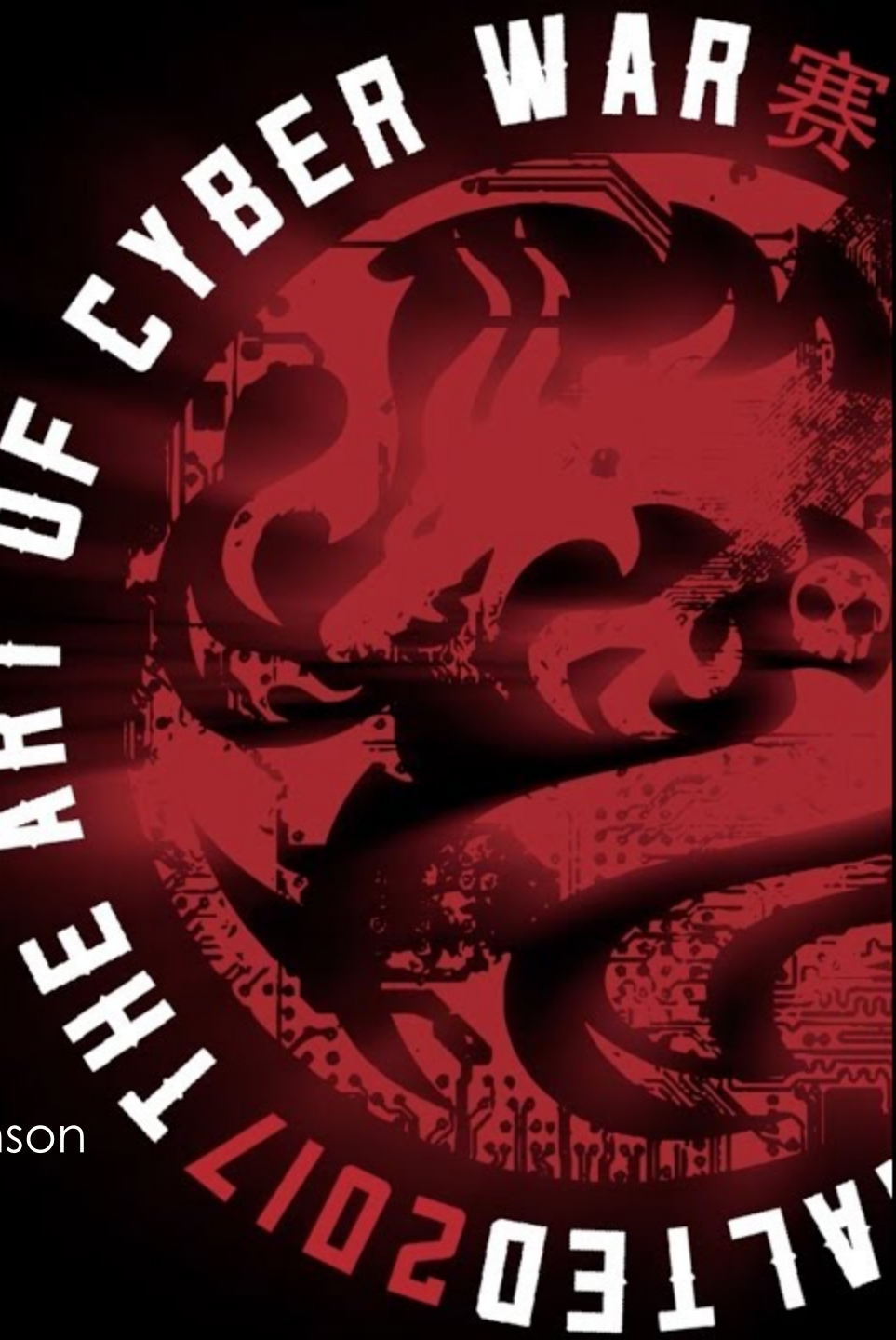
- Build Security Aware Culture
- Security Seen as Change Agent
- Security Enables Business Value at Risk (VaR)

- Integrate with Enterprise Risk Council
- Utilize Consistent Enterprise Methodology &Taxonomy
- Communicate Risk Effectively to Stakeholders
- Develop Cyber Response & Recovery Playbooks
- Cyber Insurance

* Cyber resilience is a journey, not a destination


WE CANNOT SOLVE OUR PROBLEMS
WITH THE SAME THINKING
WE USED WHEN WE
CREATED THEM
-Albert Einstein

赛博战争艺术
THE ART OF CYBER WAR
LESSONS FROM SUN TZU



John D. Johnson

john@johndjohnson.com johndjohnson.com @johndjohnson

Aligned Security: www.alignedsecurity.com