CYBER SECURITY SUMMIT 2017

Collaboration and Capabilities as Necessary Steps for Increasing Cyber Resilience

Matt Loeb, CGEIT, CAE, FASAE
Chief Executive Officer

IT's a risk-based world: The 10 most critical uncertainties companies face

1. Economic conditions may restrict growth
2. Regulatory changes and scrutiny may increase affecting products and services
3. Organizations are insufficiently prepared for cyber threats
4. Rapid speed of disruptive innovations and new technologies may outpace organizations' ability to compete or manage risk
5. Privacy, identify and information security risks are not being addressed with sufficient resources
6. Succession challenges and ability to attract top talent may limit ability to achieve operational targets
7. Anticipated volatility in global financial markets/currencies may create significant challenges
8. Org. culture may not sufficiently encourage identification and escalation of risk issues
9. Resistance to change could restrict orgs from making necessary adjustments to business model and core operations.
10. Sustaining customer loyalty and retention may be increasingly difficult as customer demographics and needs change.

Source: NACD 2017 Public Company Governance Survey

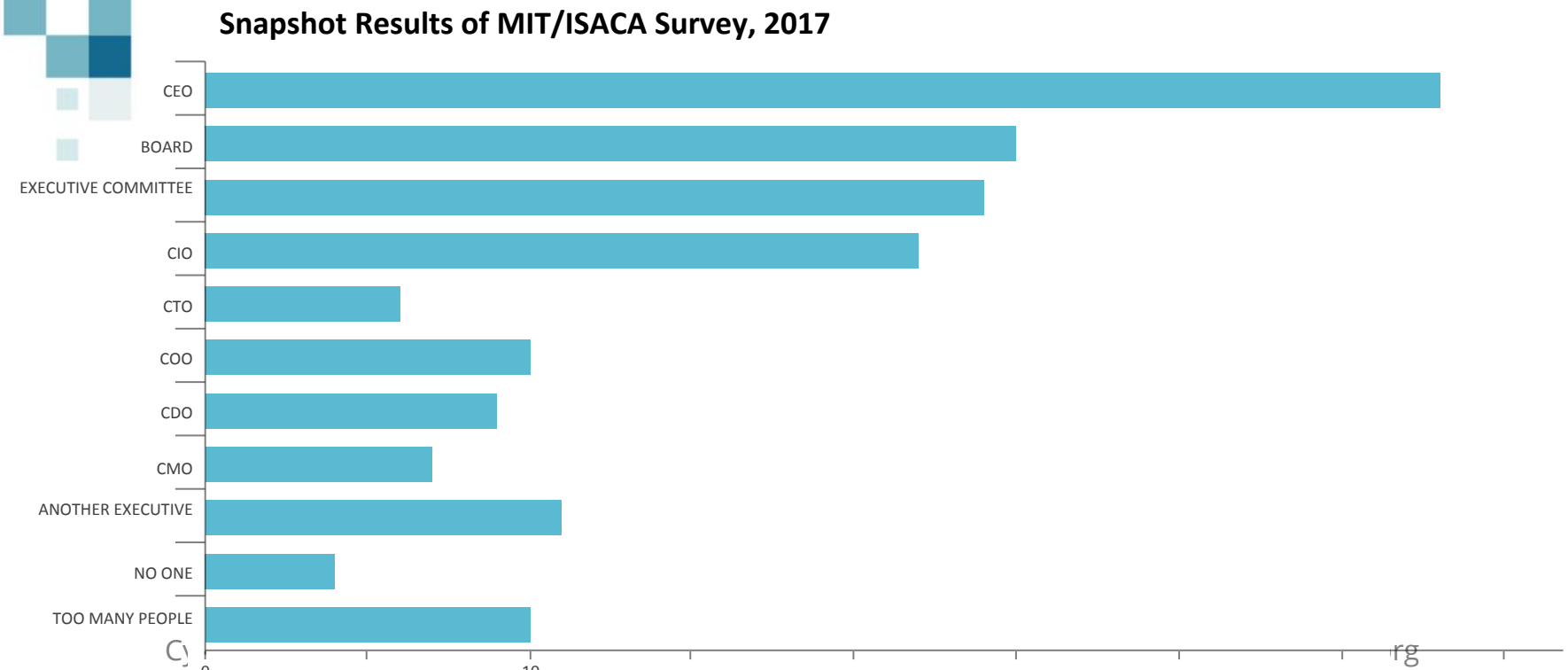
Highlighted Text is information and technology governance-related

52%

of C-suite executives think their **boards are not fully knowledgeable about the risks** the organization is taking and the measures that are in place.

Source: EY's 19th Global Information Security Survey 2016-17

Who is leading digital transformation?



“In a digital economy, the whole company is responsible for generating value from digital investments. We see three key components:”

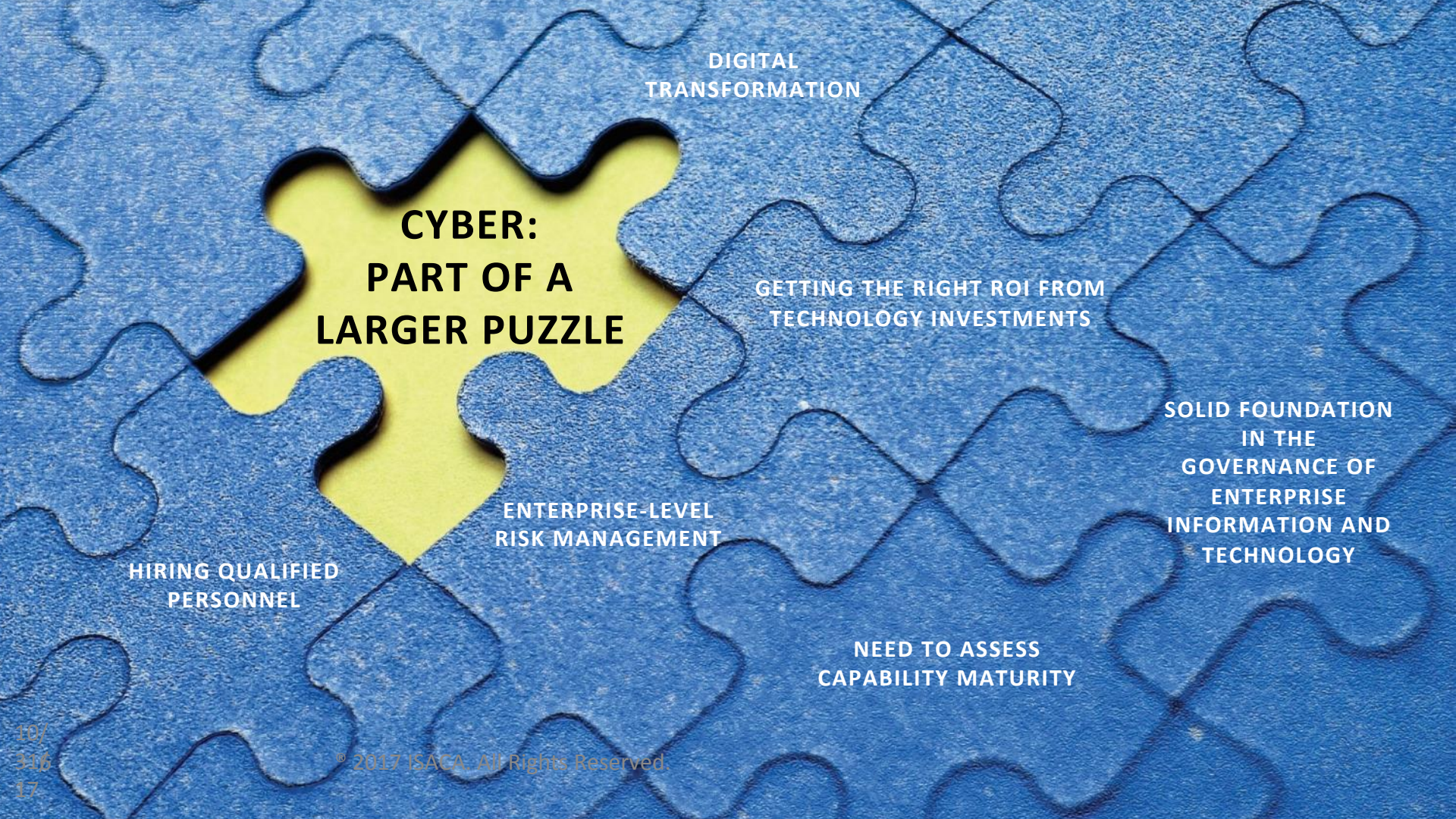
DEFENSIVE
(e.g. cyber, privacy, regulation etc.)

OVERSIGHT
(making sure the major investments and organizational change are on track)

STRATEGIC
(e.g. how will we operate in the future e.g. business models, ecosystems, partnerships).

“How good you are at each of these will predict your likely success in the digital economy.”

Dr. Peter Weill
Director, MIT Center for Information Research



87%

of board members and C-level executives have said they **lack confidence in their organization's level of cybersecurity**

Source: EY's 19th Global Information Security Survey 2016-17

57%

of enterprises have had a **recent significant cybersecurity incident,** which shows that there is still more work to do to strengthen the corporate shield.

Source: EY's 19th Global Information Security Survey 2016-17

BOARDS/C-SUITE WANT ANSWERS and ASSURANCE

ELEVATING

CYBERSECURITY RISK TO ENTERPRISE RISK

CREATING

SITUATIONAL AWARENESS

DEFINING

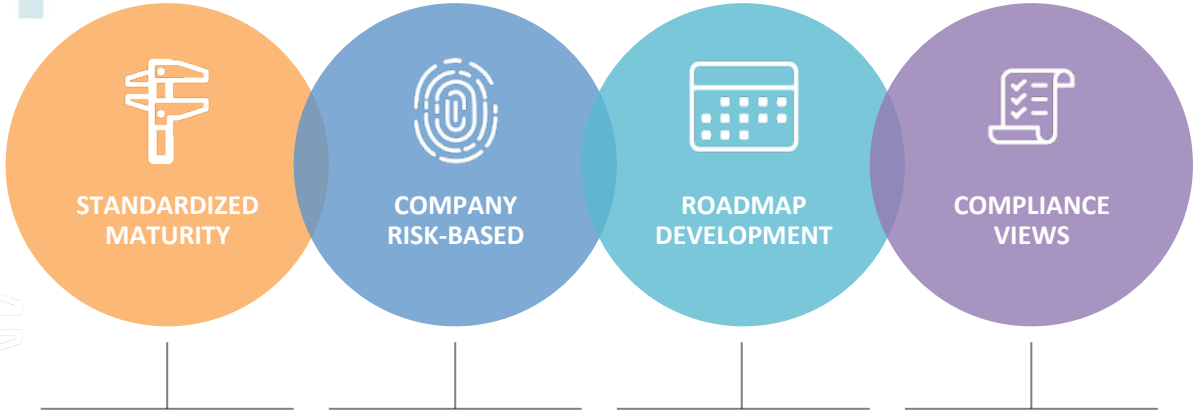
CRITICAL CAPABILITIES AND MATURING

ESTABLISHING

COMMITMENT

Cyber security capability assessment

Benefits and impact



WE PRESENT OUR RESULTS IN

BUSINESS TERMS

SIMPLE GRAPHICS TO SUPPORT BOARD COMMUNICATION

OUR

COMPREHENSIVE SCOPE

LEVERAGES LEADING FRAMEWORKS, STANDARDS AND CONTROLS


Is our organization
hiring the right people?

Hiring the Best

So…who's the better choice?

[redacted]

Cyber Security Specialist - [redacted]

Chula Vista, CA - Email me on Indeed: [redacted]

WORK EXPERIENCE

Cyber Security Specialist

[redacted] - San Diego, CA - October 2014 to Present

Conducted ACAS vulnerability scanning, application administration, and vulnerability analysis.
• Responsible for developing and modifying scan policies in Security Center

• Responsible for monitoring enterprise vulnerability status, vulnerability identification and analysis, patching and vulnerability mitigation, incident detection, compliance reporting.

• Ensure information assurance by transmitting secure data between classified systems; perform ethical hacking, malware reverse engineering, penetration testing, and Certification and Accreditation (C&A) within Security Operations Center (SOC) environment.

• Composed technical manuals, installation documents, installation progress updates, and incident response plans to enhance system security documentation.

[redacted]

Cyber Information Assurance Analyst [redacted]

Suffolk, VA - Email me on Indeed: [redacted]

Authorized to work in the US for any employer

WORK EXPERIENCE

Cyber Information Assurance Analyst

[redacted] - [redacted] - January 2015 to Present

CompTIA Security + Professional
Current Secret Security Clearance
Pursuing Certified Information System Security professional (CISSP)

Recruited to establish enterprise-wide information-security program; oversee [redacted] efforts to identify and evaluate all critical systems. Information Assurance Analyst excellent at planning, implementing, upgrading and monitoring security measures for protecting computer networks and information. Ensure appropriate security controls are in place. Provide leadership and framework to appropriately analyze needs and respond to critical security issues. Capture, test and analyze data for all new functionality being introduced into software and tools controlling the weapon systems. Document corrective action, recommend remediation strategy, and collaborate with external developers to ensure change requests are implemented into new system builds.

Time Is (Not Always) On Our Side

- In cybersecurity, 90 days is a lifetime…
- …but 180 days is an eternity…
- **And both time frames are unacceptable**

Fewer (Qualified) Applicants

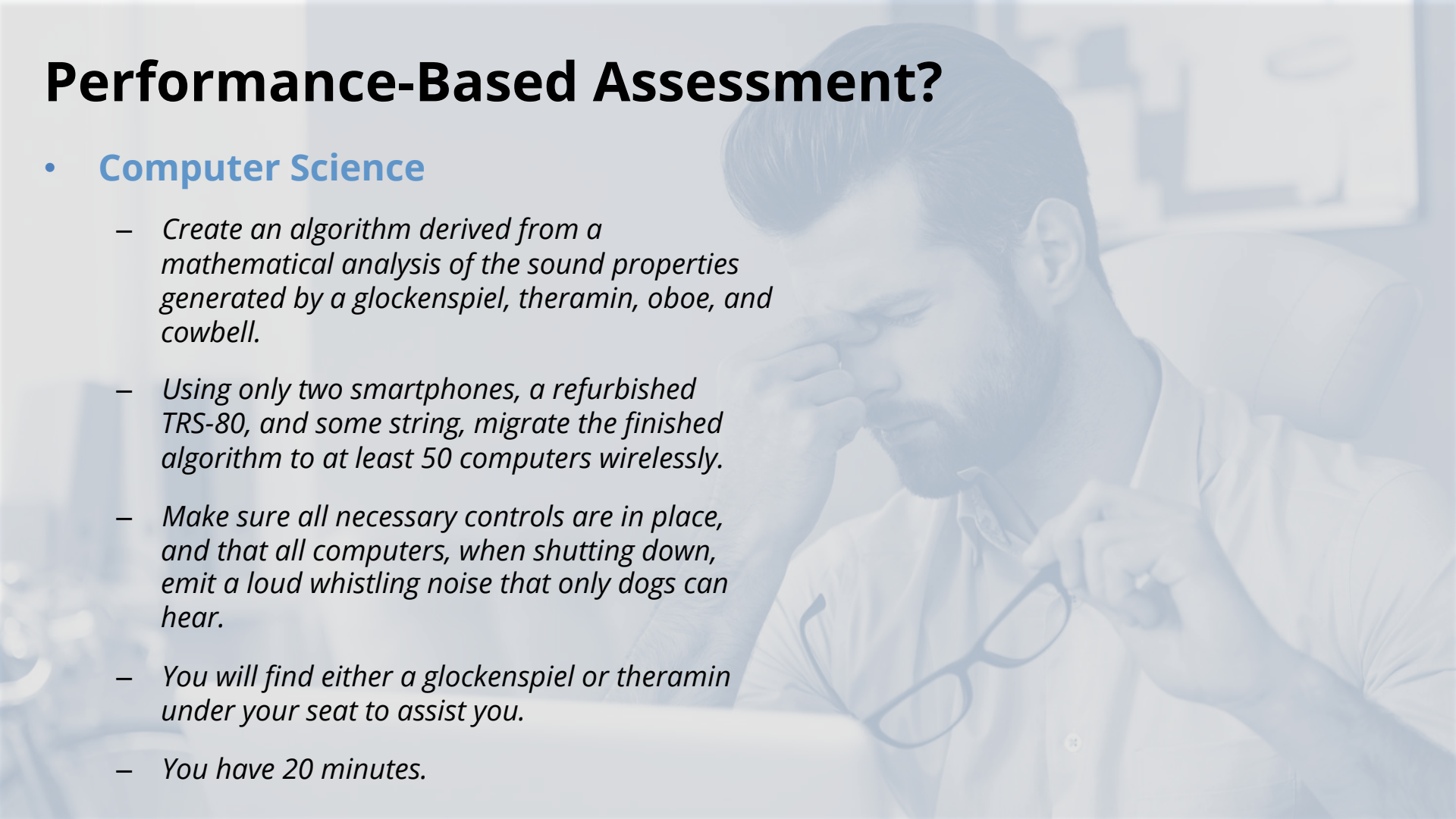
- When we do get applicants, are they qualified to safeguard our enterprise?

55%

SAY PRACTICAL HANDS-ON EXPERIENCE is the most important qualification for a cyber security candidate.

Performance-Based Assessment?

- **Computer Science**
  - *Create an algorithm derived from a mathematical analysis of the sound properties generated by a glockenspiel, theramin, oboe, and cowbell.*
  - *Using only two smartphones, a refurbished TRS-80, and some string, migrate the finished algorithm to at least 50 computers wirelessly.*
  - *Make sure all necessary controls are in place, and that all computers, when shutting down, emit a loud whistling noise that only dogs can hear.*
  - *You will find either a glockenspiel or theramin under your seat to assist you.*
  - *You have 20 minutes.*

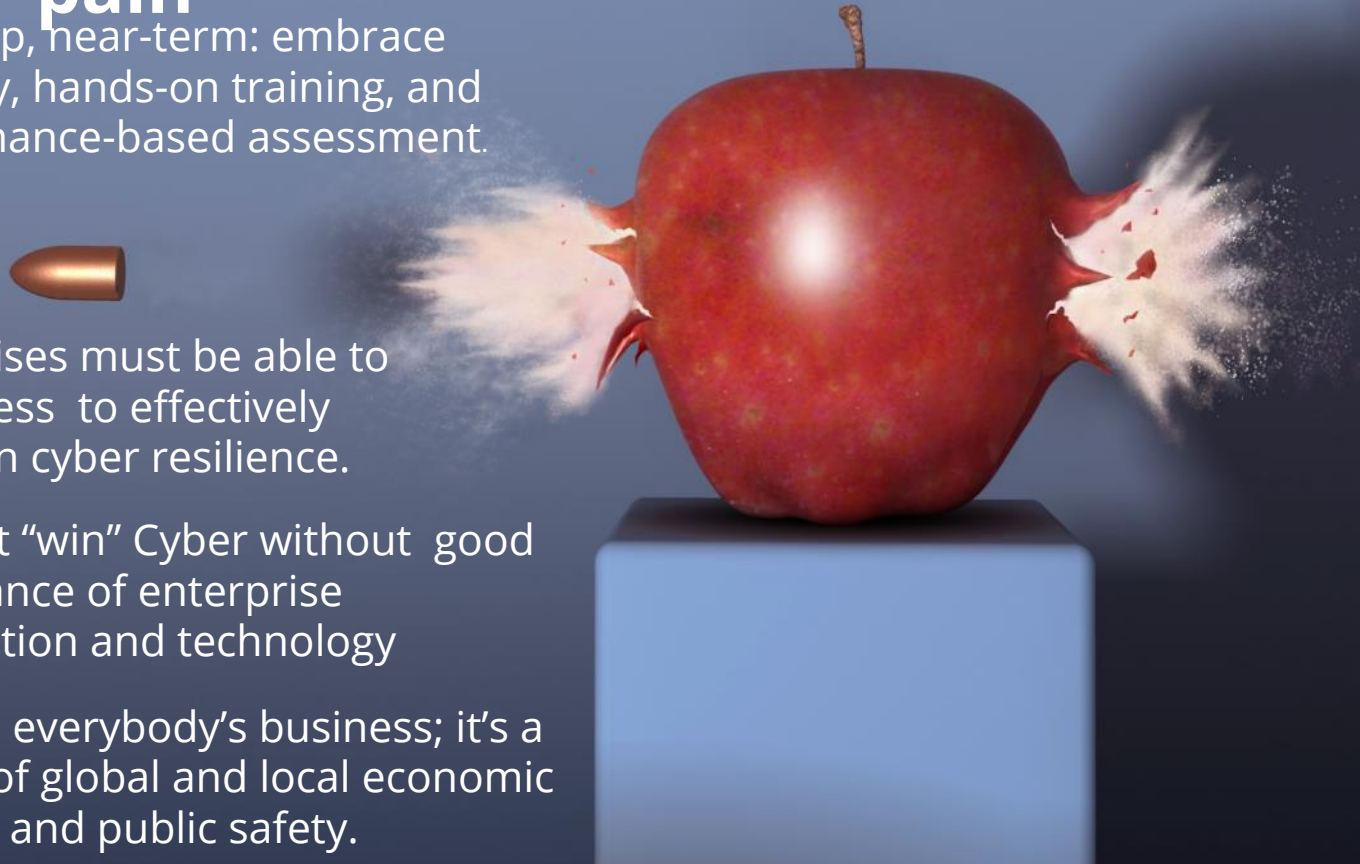


Safeguarding Your Enterprise

When choosing those who will defend your organization… choose wisely.

The pace of change creates the pain

- Skills gap, near-term: embrace diversity, hands-on training, and performance-based assessment.



- Enterprises must be able to self-assess to effectively maintain cyber resilience.
- We can't "win" Cyber without good governance of enterprise information and technology
- Cyber is everybody's business; it's a matter of global and local economic security and public safety.

THANK YOU

Questions/Comments

Matt Loeb, CGEIT, CAE
Chief Executive Officer
mloeb@isaca.org
@mattloeb