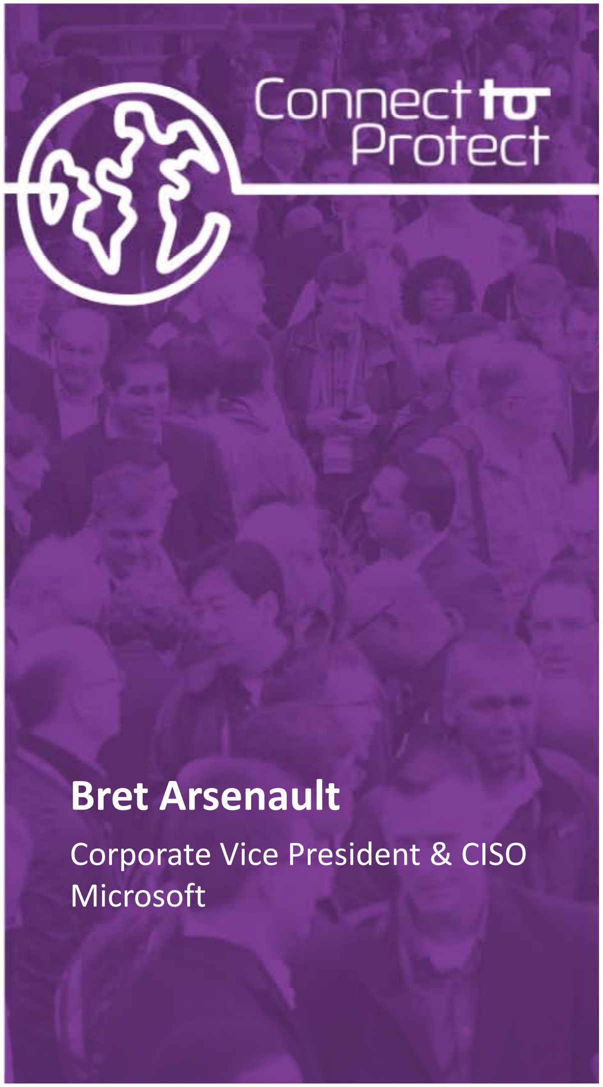
RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center



Connect to Protect

SESSION ID: **CXO-T11**

Bringing Cybersecurity to the Boardroom

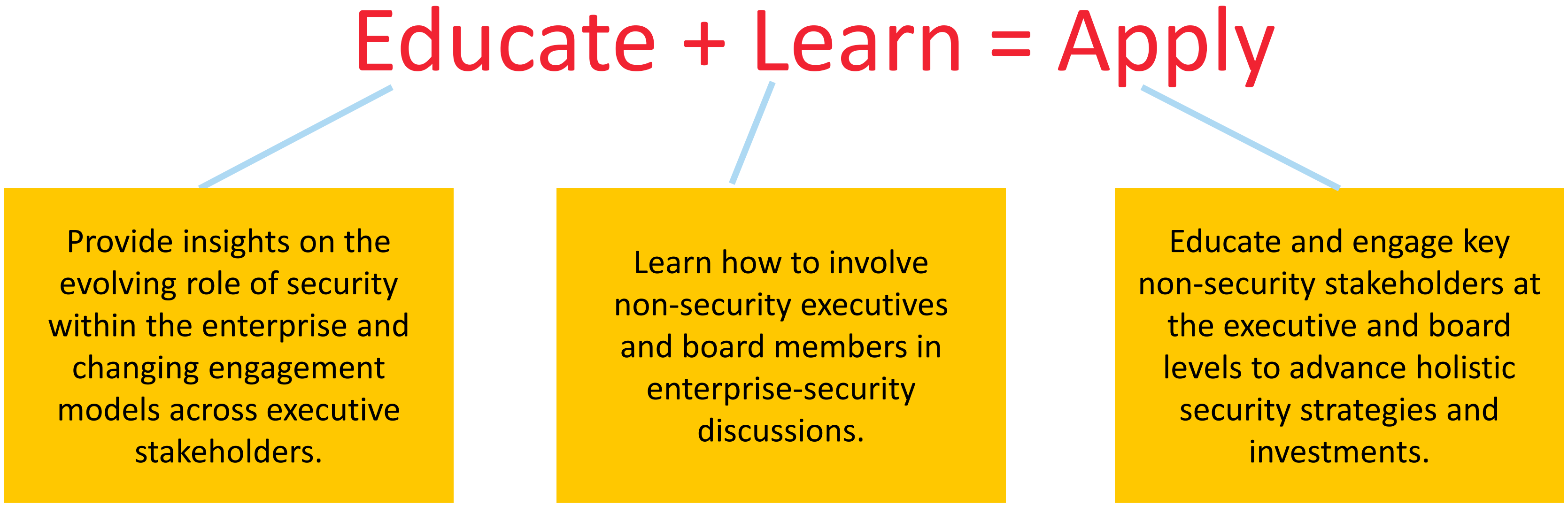
Bret Arsenault

Corporate Vice President & CISO
Microsoft

#RSAC

Apply Slide

Complete the "equation" for attendees:



Educate + Learn = Apply

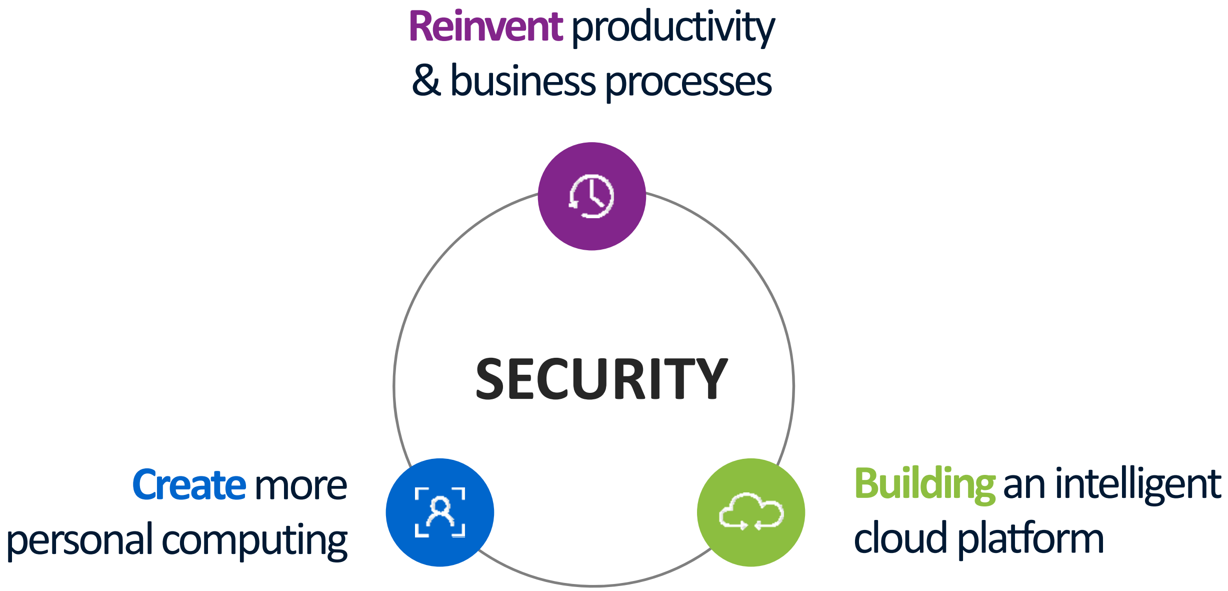
Provide insights on the evolving role of security within the enterprise and changing engagement models across executive stakeholders.

Learn how to involve non-security executives and board members in enterprise-security discussions.

Educate and engage key non-security stakeholders at the executive and board levels to advance holistic security strategies and investments.

THE INTERVIEW

How Microsoft Approaches Security



Reinvent productivity & business processes

SECURITY

Create more personal computing

Building an intelligent cloud platform

Microsoft IT Scope and Our Workforce

THE IT ENVIRONMENT:

Multi-generational

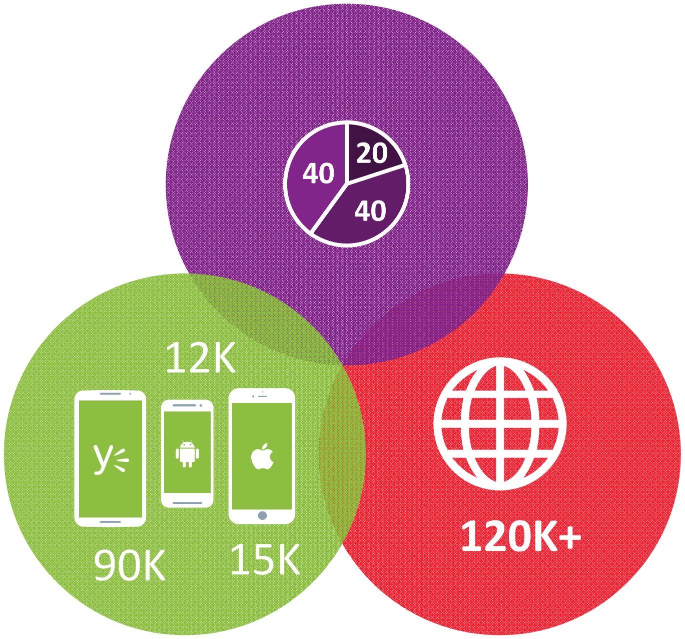
- 20% Millennial, 40% Boomers, 40% Gen X'ers

Global

- 120,000+ employees

Connected

- 325,000 devices sync via Exchange Active Sync



Security Principles

CORE
PROTECTION PRINCIPLES

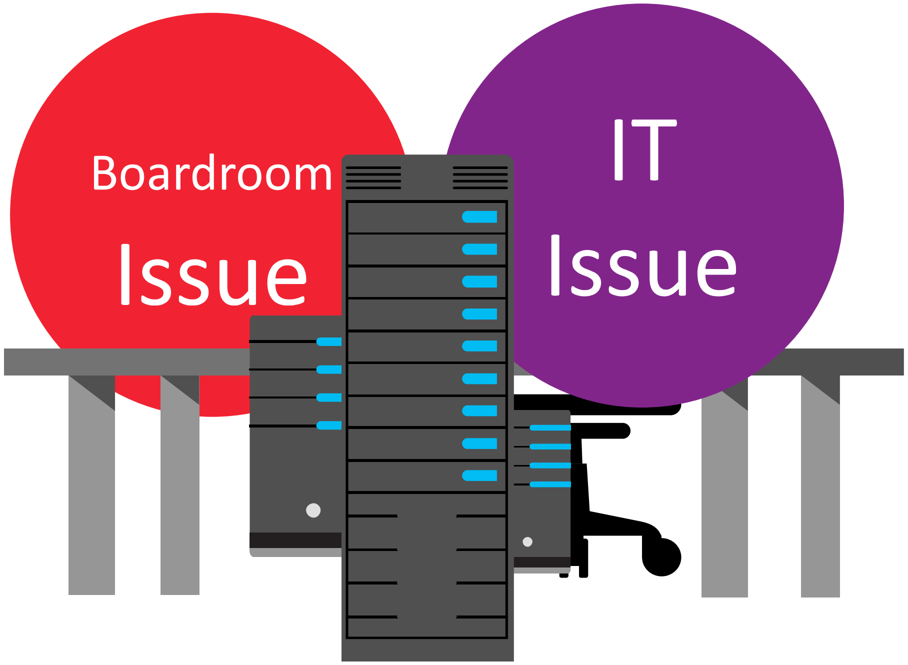
- Protect customer data
- Ensure device integrity
- Protect the supply chain
- Protect our intellectual property

Security Landscape: Snapshot

Security compromises of well-known retail brands and businesses are capturing media attention **due to:**

- Scale of compromises
- Laws requiring disclosure related to breaches of customer data
- Political motivation of malicious actors

Security has Transcended from...to an...



Boardroom Issue

IT Issue

What’s Influencing The Board

INCREASING NUMBER OF HIGH PROFILE BREACHES

EMERGING WAVE OF CLASS ACTION SUITS FROM CONSUMERS AND SHAREHOLDERS

INCREASED REGULATORY ATTENTION, STRUCTURE AND ACTIVITY

What’s Influencing The Board

Increased Activity and Regulation from Securities Exchange Commission and Federal Trade Commission

INCREASING ENFORCEMENT OF CYBERSECURITY REQUIREMENTS

Boardroom

BRINGING ACTIONS AGAINST COMPANIES EXPERIENCING DATA BREACHES

Strategic Planning Assumptions

NIST Cybersecurity Framework Adoption

By 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from the current 30% in 2015.

Gartner Security & Risk Management Summit Presentation, Using the NIST Cybersecurity Framework, Khushbu Pratap & Earl Perkins, 8-11 June 2015

By 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from the current 30% in 2015.

Arguments in Favor of the Assumption

- It is not too prescriptive nor too vague.
- Serves as a tool to communicate to senior management and board members.
- Is being revised with inputs from public and private sectors.
- Non-U.S. entities are inspired for mitigating cyberthreats.

Arguments that are Inhibitors to the Success of the Assumption

- Excess. Addition to existing compliance obligations.
- Gap in management of OT and IT not addressed if mapping not taken seriously.
- Rate of cyber incidents will leave no time for proactive risk management.
- A permutation of a subset of the five referenced standards is used, not considering the framework

Gartner Security & Risk Management Summit Presentation, Using the NIST Cybersecurity Framework, Khushbu Pratap & Earl Perkins, 8-11 June 2015

Recommendations & Guidance

SEC Guidance

- Cybersecurity as an assigned area for the entire Board or a Board committee
- Review annual budget for privacy and security programs
- Ensure a governance structure has been created to address cybersecurity
- Ensure good cyber incident response plan to address potential breaches

Both

Industry Guidance

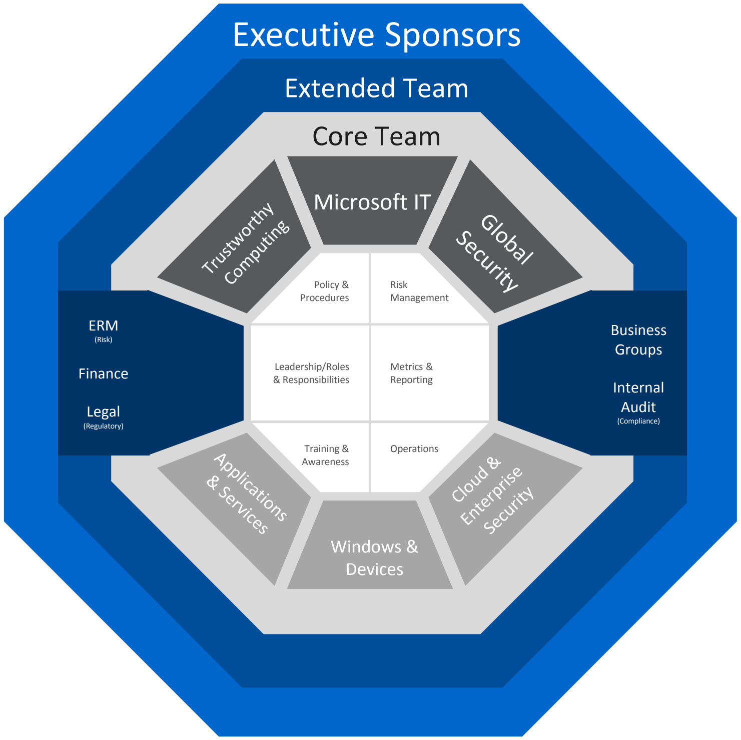
- Audit or Risk Committee common home for Board cybersecurity oversight
- Review NIST and other security standards for best practices and align to the standards
- Ensure good cyber incident response plan to address potential breaches

IRMC

Information Risk Management Council

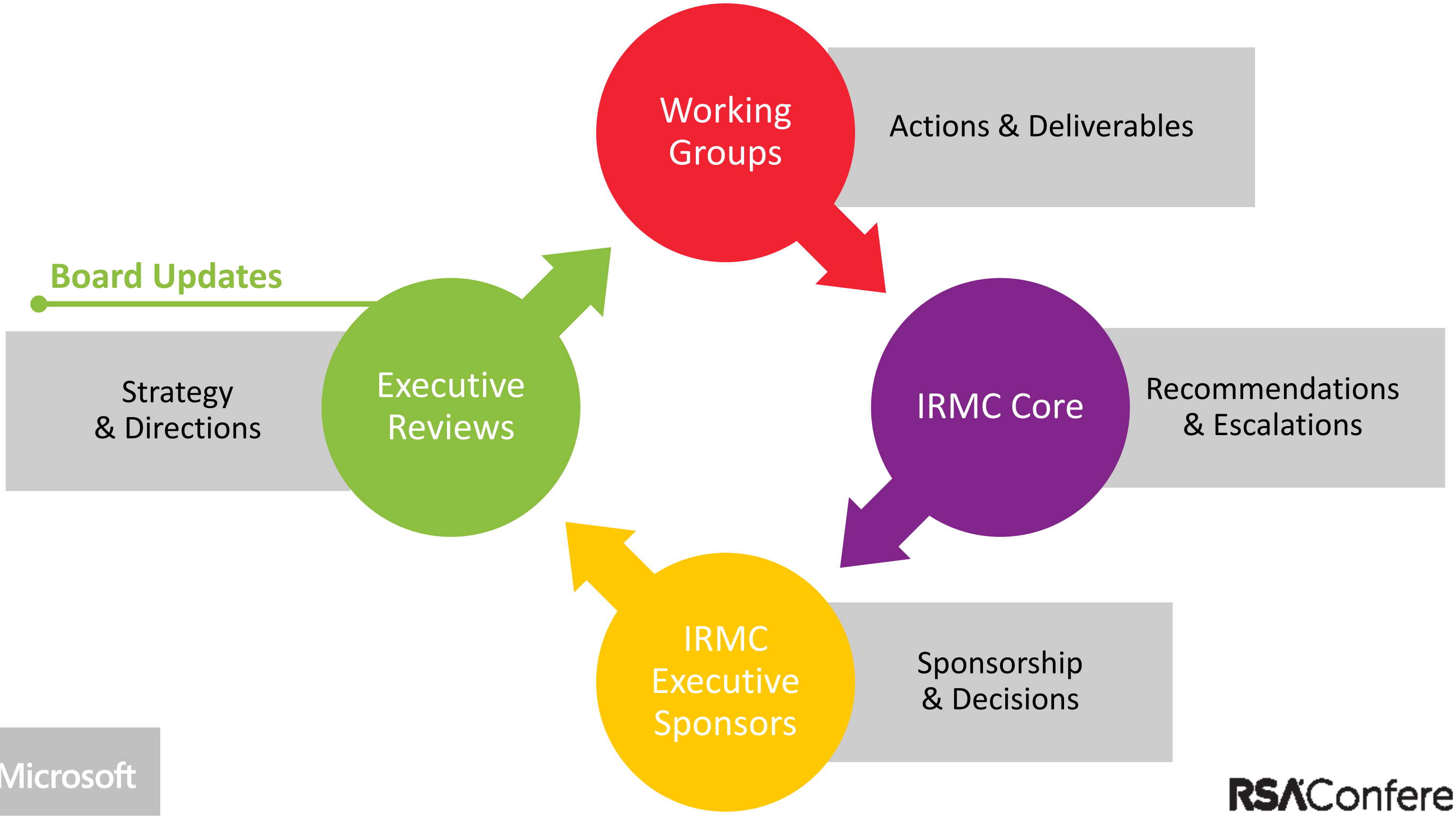
How do we manage enterprise risk?

The mission of the Information Risk Management Council (IRMC) program is to enable a risk-based approach for managing information security, physical security, and customer and employee privacy related matters.



#RSAC

IRMC Engagement



Working Groups

Actions & Deliverables

IRMC Core

Recommendations & Escalations

IRMC Executive Sponsors

Sponsorship & Decisions

Executive Reviews

Strategy & Directions

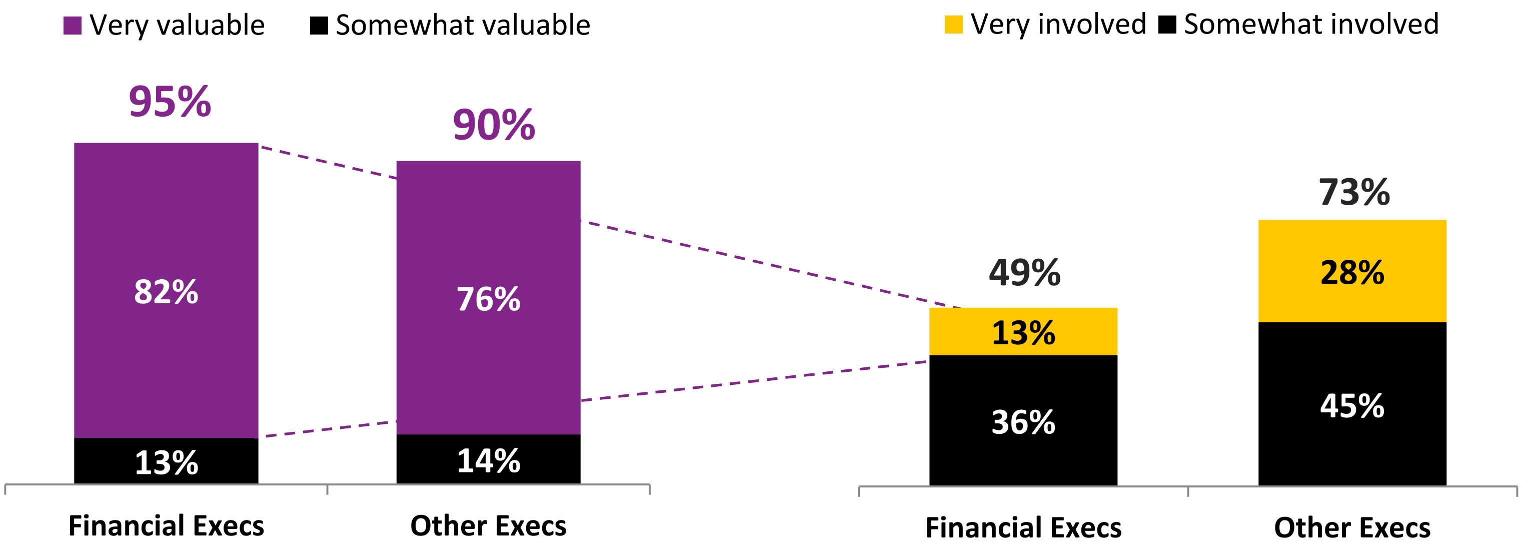
Board Updates

Microsoft

RSAConference2016

Financial Executives place a higher value on information security (I.S), but an involvement gap exists

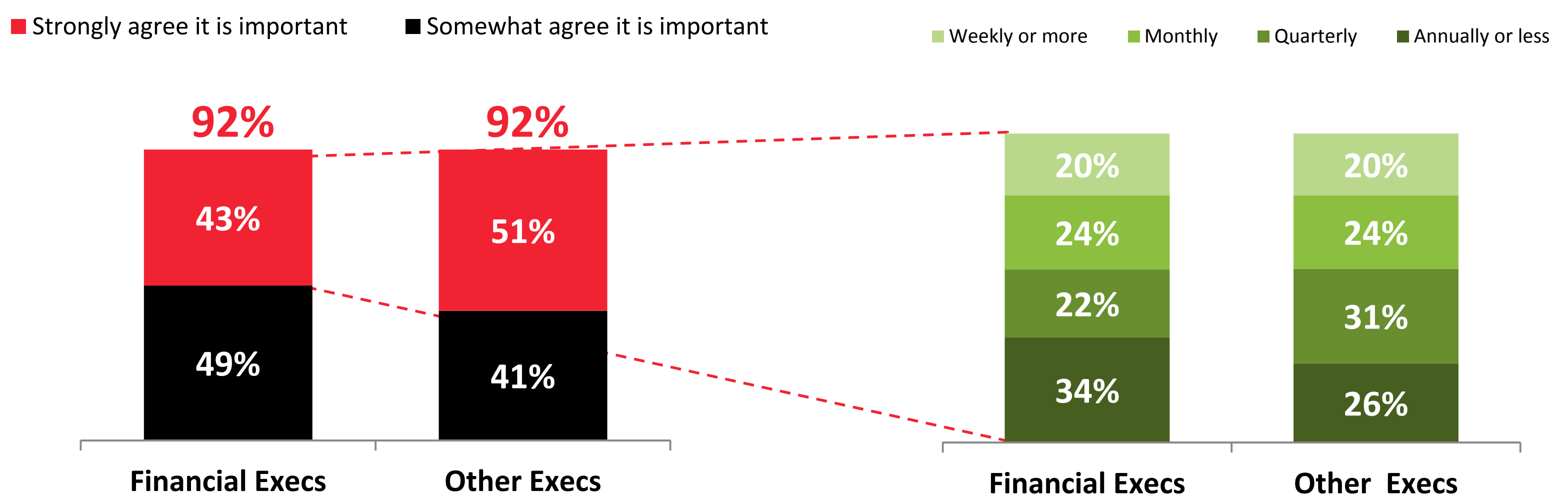
VALUE OF INFORMATION SECURITY > INVOLVEMENT IN INFORMATION SECURITY



Integration is recognized as important, but in practice, direct communication is often very infrequent

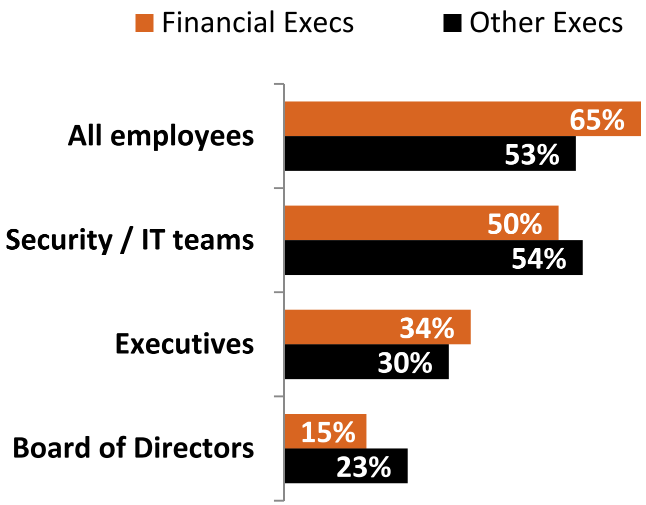
IMPORTANCE OF DEPARTMENT INTEGRATION WITH I.S.

FREQUENCY OF COMMUNICATION WITH I.S. LEADER



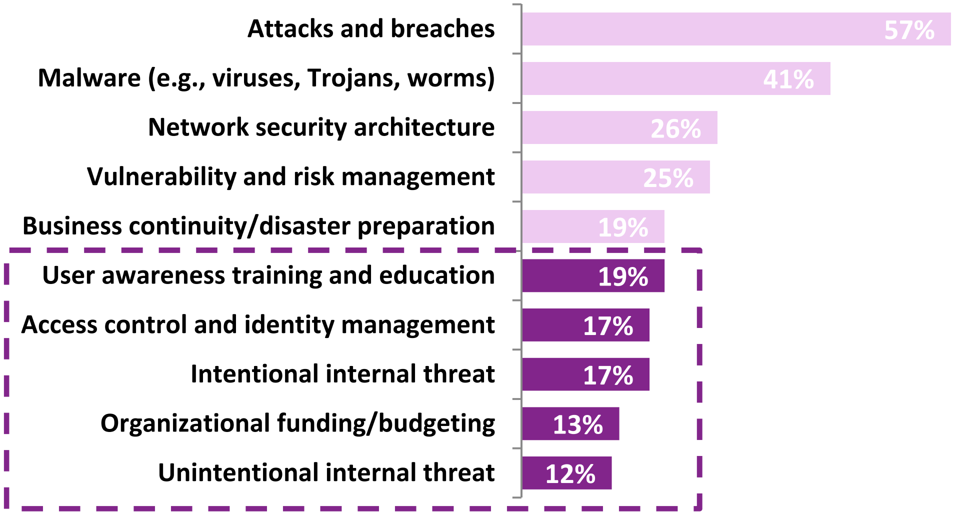
Financial executives see security as a shared responsibility, yet internal threats are less of a concern

RESPONSIBILITY FOR INFORMATION SECURITY

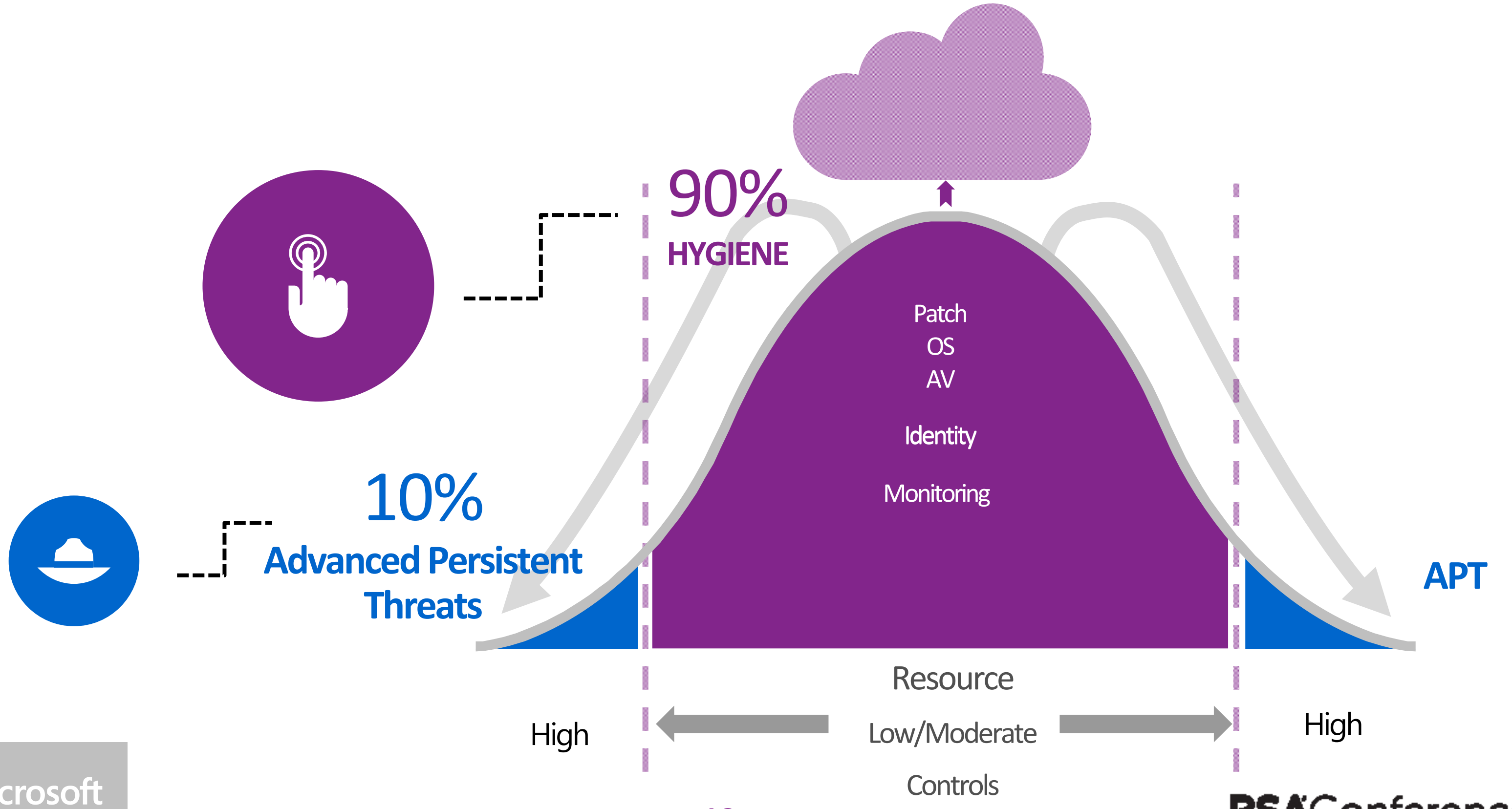


TOP INFORMATION SECURITY CONCERNS

(Shown: % Top Three Choice among Financial Execs)



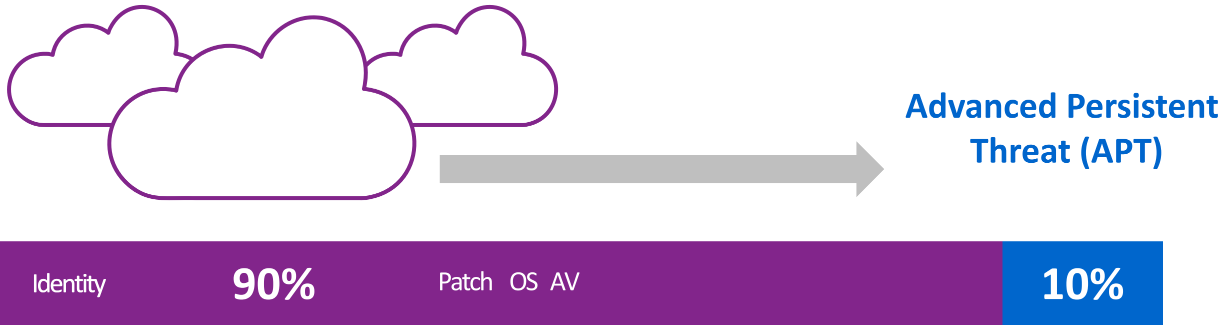
Effective Risk Mitigation



Effective Risk Mitigation

The Risk Environment

90% incidents could be preventable with Hygiene, freeing up resources to combat **APT attacks.**



Advanced Persistent Threat (APT)

Monitoring Identity **90%** Patch OS AV

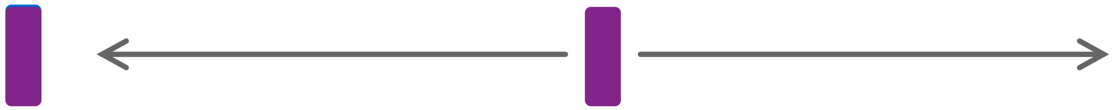
10%

Hygiene

HONOR
THE **PAST**

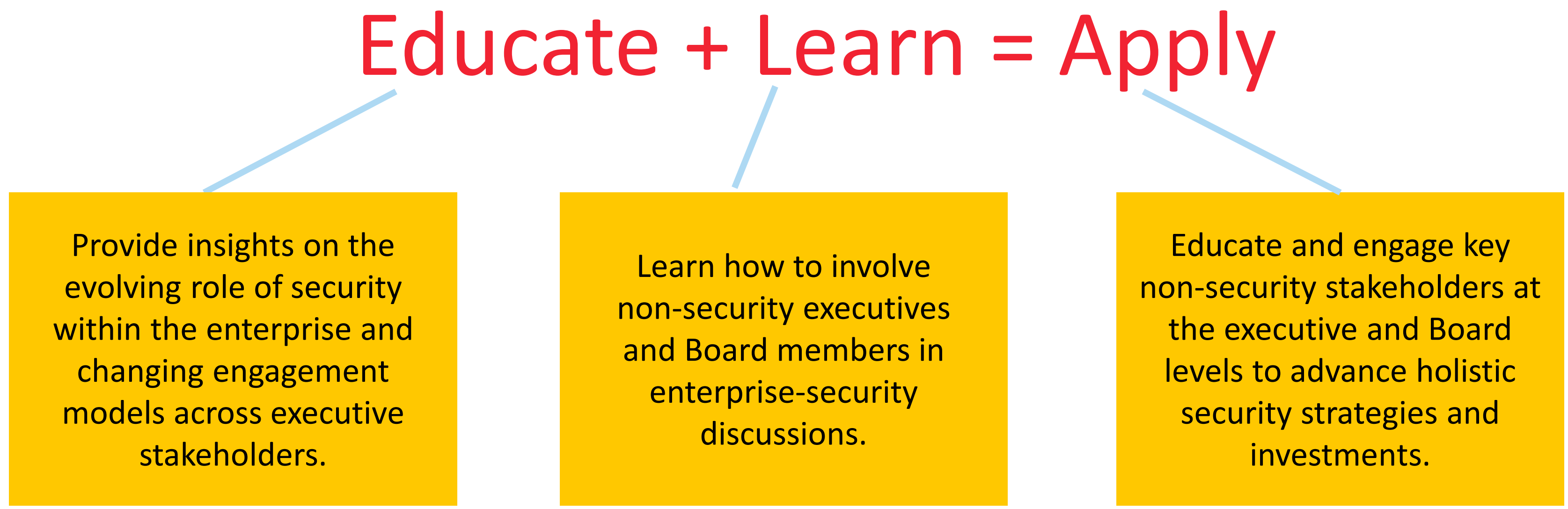
BE HONEST ABOUT
THE **PRESENT**

BUILD FOR
THE **FUTURE**



Apply Slide

Complete the “equation” for attendees:



Educate + Learn = Apply

Provide insights on the evolving role of security within the enterprise and changing engagement models across executive stakeholders.

Learn how to involve non-security executives and Board members in enterprise-security discussions.

Educate and engage key non-security stakeholders at the executive and Board levels to advance holistic security strategies and investments.

Questions?