10th ANNUAL
CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00-9:10	Dr. Deanne Snavely, Dean, College of Natural Sciences and Mathematics	*Opening Remarks*
9:10-9:20	Dr. Francisco E. Alarcón, Acting chair, Department of Computer Science	*Welcome Message*
9:20-9:30	Dr. Waleed Farag, Professor of Computer Science and Director, Institute for Cybersecurity at IUP	*Event history, ICS work and recent achievements, and logistics.*
9:30-10:20	Dr. James Joshi, Professor, Department of Informatics and Networked Systems, School of Computing and Information, University of Pittsburgh	*Insider Threats: Challenges and Mitigation Approaches*
10:20-10:35	AM Break	
10:35-11:25	Mr. Skip Irwin, Account Executive for Wombat Security Technologies	*The State of Security Awareness and Education: Phishing and Beyond*
11:25-12:50	Lunch Break	
12:50-1:00	Dr. Tim Moerland, IUP's Provost and Vice President for Academic Affairs	*Provost's Remarks*
1:00-1:50	Dr. Isaac Porche, Director, Acquisition and Development Program, Homeland Security Operational Analysis Center (HSOAC), RAND Corporation	*Cyber Power and the Reserve Component*
1:50-2:00	PM Break	
2:00-2:50	Mr. Joe Harford, President and Founder, Reclamere	*The 2018 Cyber Security Employment Landscape and You*
2:50-3:00	PM Break	
3:00-3:50	Mr. David Brown, CISSP, PMP, Manufacturing Information Security Business Strategist, Business Complete Solutions	*The Cybersecurity Professional's Current and Future Challenges*
3:50-4:00	Dr. Waleed Farag, Director, Institute for Cybersecurity at IUP	*Conclusions*

before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Isaac's latest publication, Cyber Power Potential of the Army's Reserve Component, focuses on research conducted on how to train, manage, and develop the Army's Cyber force.

Mr. Joe Harford, President and Founder, Reclamere

Joe Harford, President and Founder, Reclamere, a 16-year old information security company located in Central Pennsylvania that serves clients in highly regulated market sectors. The company has been providing its' clients with information security solutions throughout the Mid-Atlantic region. Reclamere works with clients of all sizes and stages of the security maturity model.

Mr. David Brown, CISSP, PMP, Manufacturing Information Security Business Strategist, Business Complete Solutions

David C. Brown, PMP, CISSP, is the founder of Business Complete Solutions®. He shows leaders of manufacturing companies how to grow their business, and improve their competitiveness while they manage the risk of cyber-attacks and Compliance penalties.

He has more than twenty-five years experience in manufacturing and seventeen in various cybersecurity roles. He has filled leadership positions in diverse engineering, consulting, and management positions at a wide variety of companies and industries.

He specializes in using cybersecurity tools, techniques, and procedures to enable companies to innovate and improve business profits.

https://www.businesscompletesolutions.com/

TITLES AND ABSTRACTS

Dr. James Joshi, Professor, University of Pittsburgh

Title: ***Insider Threats: Challenges and Mitigation Approaches***
Abstract: Insider threats pose as an increasingly challenging issue that has significant potential impacts on organizations. Detection, mitigation and/or prevention of insider attacks present complex challenges while the boundary between an insider and an outsider within the context of an organizational information system is becoming increasingly blurry because of the immense interconnectivity among devices and applications, and organizational information systems; this is further aggravated by evolving and emerging technologies such as Cloud computing and the Internet of Things (IoT). In this talk, I will discuss various challenges, potential mitigation approaches and our ongoing research efforts related to tackling insider threats.

Mr. Skip Irwin, Account Executive for Wombat Security Technologies

Title: ***The State of Security Awareness and Education: Phishing and Beyond***
Abstract: This session will provide a comprehensive overview of the different threats facing end users today and the steps proactive organizations are taking to protect themselves. In addition to phishing, it will highlight lesser known, but equally as dangerous threat vectors such as social engineering, mobile security, and ransomware. Skip will also discuss why an effective security plan must address a full scope of threats and share best practices on how to create an actionable security awareness and training program to effectively change behavior and reduce risk.

Dr. Isaac Porche, Director, Acquisition and Development Program, Homeland Security Operational Analysis Center (HSOAC), RAND Corporation

Title: ***Cyber Power and the Reserve Component***
Abstract: The military services are formalizing and bolstering their contribution to the nation's cyber force, known as the U.S. Cyber Command Cyber Mission Force. As part of a Total Force approach, the Army is considering using both active component and reserve component personnel to fill the Cyber Mission Force and other requirements in support of Army units. This presentation will discuss ways in which these soldiers can be leveraged to conduct Army cyber operations as well as the broader challenges and opportunities that the use of reserve component personnel presents.

Mr. Joe Harford, President and Founder, Reclamere

Title: ***The 2018 Cyber Security Employment Landscape and You***
Abstract: OK, so you have that prized information security degree, solid internship experience, and your first job offer—now what? The now what question is one that has plagued graduates for decades. This presentation is not about your short-term savings plan, 401K strategy, or winning real estate advice, although that would be helpful. Rather this speaker will explain to you how important organizational culture, attitude, and a PIVOT mindset will differentiate you from your other professional colleagues.

Mr. David Brown, CISSP, PMP, Manufacturing Information Security Business Strategist, Business Complete Solutions

Title: ***The Cybersecurity Professional's Current and Future Challenges***
Abstract: The cybersecurity field is extremely complex and fast moving. Each year cybercriminals victimize thousands of large and small companies. David C. Brown, PMP, CISSP, founder of Business Complete Solutions, will discuss some of the current and future challenges facing cybersecurity professionals as they endeavor to protect their company and their career.

For more information about Cybersecurity Day at IUP, please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at *farag@iup.edu*, 724-357-7995.

THE 10TH ANNUAL

CYBERSECURITY DAY AT IUP

OCTOBER 26, 2017

STOUFFER AUDITORIUM

IUP MAIN CAMPUS

CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00-9:10	Dr. Deanne Snavely, Dean, College of Natural Sciences and Mathematics	*Opening Remarks*
9:10-9:20	Dr. Francisco E. Alarcón, Acting chair, Department of Computer Science	*Welcome Message*
9:20-9:30	Dr. Waleed Farag, Professor of Computer Science and Director, Institute for Cybersecurity at IUP	*Event history, ICS work and recent achievements, and logistics.*
9:30-10:20	Dr. James Joshi, Professor, Department of Informatics and Networked Systems, School of Computing and Information, University of Pittsburgh	*Insider Threats: Challenges and Mitigation Approaches*
10:20-10:35	AM Break	
10:35-11:25	Mr. Skip Irwin, Account Executive for Wombat Security Technologies	*The State of Security Awareness and Education: Phishing and Beyond*
11:25-12:50	Lunch Break	
12:50-1:00	Dr. Tim Moerland, IUP's Provost and Vice President for Academic Affairs	*Provost's Remarks*
1:00-1:50	Dr. Isaac Porche, Director, Acquisition and Development Program, Homeland Security Operational Analysis Center (HSOAC), RAND Corporation	*Cyber Power and the Reserve Component*
1:50-2:00	PM Break	
2:00-2:50	Mr. Joe Harford, President and Founder, Reclamere	*The 2018 Cyber Security Employment Landscape and You*
2:50-3:00	PM Break	
3:00-3:50	Mr. David Brown, CISSP, PMP, Manufacturing Information Security Business Strategist, Business Complete Solutions	*The Cybersecurity Professional's Current and Future Challenges*
3:50-4:00	Dr. Waleed Farag, Director, Institute for Cybersecurity at IUP	*Conclusions*

BIOGRAPHICAL INFORMATION

Dr. James Joshi, Professor, Department of Informatics and Networked Systems, School of Computing and Information, University of Pittsburgh

James Joshi is a professor of the School of Computing and Information at the University of Pittsburgh, and the director and co-founder of the Laboratory of Education and Research on Security Assured Information Systems (LERSAIS), which has been designated as a Center of Academic Excellence in Information Assurance and Cyber Defense Education and Research (CAE and CAE-R). He is an elected fellow of the Society of Information Reuse and Integration (SIRI) and a senior member of the IEEE and the ACM. His research interests include access control models, security and privacy of distributed systems, trust management, network security, and security and privacy services in cloud computing, critical infrastructures, and social networking environments. He is a recipient of the US NSF-CAREER award in 2006. He has served as program co-chair and/or general co-chair of several international conferences/workshops. He currently serves as the steering committee chair of IEEE CIC. He was a founder and co-Editor-in-chief of EAI Endorsed Transactions on Collaborative Computing. Currently, he is the EiC of the IEEE Transactions on Services Computing. He had also served in or is in the editorial board of several international journals. His work has been recognized with Best Paper award in ACM CODASPY 2011 and BigData Congress in 2017, and Best Student Paper award in ACM SIGSPATIAL 2011. He is a co-editor of the book titled "Information Assurance: Dependability and Security of Networked Systems" published in 2007. He has published over 120 articles as book chapters and papers in journals, conferences and workshops, and has served as a special issue editor of several journals including Elsevier Computer & Security, ACM TISSEC (now TOPS), Springer MONET, IJCIS, and Information Systems Frontiers.

Mr. Skip Irwin, Account Executive for Wombat Security Technologies

Skip Irwin, Account Executive for Wombat Security Technologies, a leading provider of security education that changes employee behavior. Founded in 2008, Wombat's Security Education Platform includes integrated knowledge assessments, a library of simulated attacks, and interactive training modules.

Dr. Dr. Isaac Porche, Director, Acquisition and Development Program, Homeland Security Operational Analysis Center (HSOAC), RAND Corporation

Isaac is a senior engineer at the RAND Corporation, where he currently serves as the Director of the Acquisition and Development Program in the Homeland Security Operational Analysis Center (HSOAC). As the director, Isaac overseas a wide range of projects supporting the Department of Homeland Security and its components. He joined RAND in 1998 after graduating from the University of Michigan with a Ph.D. in electrical engineering. He has led research projects for the U.S. Navy, U.S. Army, the Department of Homeland Security (DHS), the Joint Staff, and the Office of the Secretary of Defense. He has served on the U.S. Army Science Board supporting a number of its cyber related panels. At the Institute of Politics and Strategy at Carnegie Mellon University, Isaac serves as an adjunct instructor, where he teaches a graduate class titled Policy and Technology of Cyberwar. He has authored numerous RAND publications, peer-reviewed journal articles and conference papers. He is also a frequent contributor of op-eds and commentary for news outlets on military and science topics and has been quoted in other media outlets including National Public Radio, the San Francisco Chronicle, and the Baltimore Sun.

Isaac's areas of expertise include cybersecurity, network and communication technology, intelligence, surveillance, and reconnaissance (ISR) systems, data mining, modeling and simulation, cybersecurity, rapid acquisition processes, and operations research techniques. In 2016, he presented testimony on emerging cyber threats and implications

The Cybersecurity Professional's Current and Future Challenges

David C. Brown, PMP, CISSP
CEO/President
Business Complete Solutions
https://www.BusinessCompleteSolutions.com

Agenda

1. Why important to businesses
2. Examples
3. How did we got here
4. Concepts and Terms
5. Current & future challenges
6. Summary
7. Questions

BUSINESS COMPLETE SOLUTIONS

Not discussing

- ID theft,
- Personal security issues
- Mitigation measures

Why Important:

Loss to companies:

- Intellectual property (IP)
- Money/time/distraction 2013 $3T
- Partner and customer trust - Target
- Lost jobs - Target, Equifax
- Life threatening - Electric grid, Dams, transportation, and even cars

Examples:

- **Bots and DDOS**
  - o IoTroop may be 1 Million machines worldwide
  - oLast year Mirai 100,000 machines

- **CCleaner - Software supply chain Attack**
  - o2.7 M machines, secondary attack 23 machines in 8 countries telcoms
  - oConcept?
  - o4 weeks to discover

BUSINESS COMPLETE SOLUTIONS

- **Macs**
  - Elmedia (media player)
  - Handbrake (video transcoder)
  - FOLX (Download manager)
  - Information stealing malware

- **Ransomware**

NAYANA

  - South Korean web hosting company **Nayana** paid more than $1 million
    - 153 of Nayana's servers
    - 3,400+ websites hosted by the company
    - Many were businesses websites

-
- **BadRabbit**, Tuesday, More than half the victims were in Russia, followed by Ukraine, Bulgaria, Turkey and Japan - ESET
  - **WannaCry** (May) - 200,000
  - **NotPetya** (June)

- **IP Theft - Wind Turbine Technology**

- **American Superconductor** - Massachusetts

SINOVEL
华 锐 风 电

- **Wind turbines** China Sinoval & insider employee

BUSINESS
COMPLETE SOLUTIONS

How we got here

Did not even think about security

Speed, cost, functionality, & time to market

Terms and concepts

CIA Triad + NA

- Confidentiality
- Integrity
- Availability

+

- Non-repudiation
- Authentication

Attack types: STRIDE

- **S**poofing,
- **T**ampering,
- **R**epudiation,
- **I**nformation Disclosure,
- **D**enial of Service, and
- **E**levation of Privilege

BUSINESS COMPLETE SOLUTIONS

Attacker Steps

1. Reconnaissance,
2. Weaponization,
3. Delivery,
4. Exploitation,
5. Installation,
6. Command & Control (C2), Pivoting,
7. Actions on Objectives
   - Ransomware, exfiltration, disruption, destruction, or Bot

Current and Future Security Challenges

15. Quantum computing

- 13 billion years vs. 10 seconds
- Kills all encryption schemes

14. Machine Learning & AI

- Bad guys- application vulnerabilities
- Good guys still learning
- Can be defeated

13. Changing Attacker profile:

- Nation States - Russia, China, Iran, North Korea- fund, train and protect hackers
- Organized Crime
- Sophistication & Resources
  - It's an industry
- Low Cost and availability of hacking and Ransomware toolkits to millions
- "We are in a cyber war."

12. Expensive security tools

- Not everyone is vaccinated

11. BitCoin

- Anonymous payment system, Untraceable Source of money

10. Complexity -

- Time, budget, resources,
  - Data - Volume, Velocity, and variety -
  - Hard to analyze, classify, filter and protect

9. OSS - Open Source Software

- 180,000 OSS Projects
- 1,400 licensing types
- More than a million modules
- Tested and Secure programming?

8. API - Application Programming Interface

- 18,000 APIs (Expedia, eBay, Salesforce)
- Used in many places and companies
- Tested and Secure programming?

7. IPv4 to IPv6 Migration

- **IPv4**
  - 1981
  - 32 bit addresses

    101.234.012.044
  - 4 billion addresses
- **IPv6**
  - 1998
  - 128 bit address space

    FE80:0000:0000:0000:0202:B3FF:FE1E:8329
  - 34x10^37 addresses

6. Legacy Hardware & Software -

- Still in use since 1960s
- Vulnerable
- Not patched
- Not maintainable
- Brittle
- No documentation, compliers, hardware

5. Threat Intelligence faster, accurate and growing utilization

4. Borderless Networking

- GE 600 offices directly to internet, not corporate network
- Saves millions of dollars maintenance, hardware and software

3. IoT explosion

- **2020 26 Billion** devices connected to networks
- Complexity, vulnerabilities, management, ...

2. New sense of urgency in industry and governments

1. EUBA

- **E**ntity, **U**ser **B**ehavioral **A**nalysis
  - Users, networks and machines

Some Never Learn - Continuing Issues

Ignorance

1. "I don't need cybersecurity, I have cyber insurance."
2. "I am too small for attackers."
3. "IT handles our cybersecurity."

Summary

2021 -

Worldwide Cybercrime damages
- $6 trillion annually

Questions?

David C. Brown, PMP, CISSP
CEO/President
Business Complete Solutions
(412) 357-0266

Dave@BusinessCompleteSolutions.com
https://www.BusinessCompleteSolutions.com

BUSINESS COMPLETE SOLUTIONS

RECLAMERE

DATA SECURITY EXPERTS

Cybersecurity Day

The 2018 Cyber Security Employment Landscape and You

NOW WHAT?

- Organizational Culture
- Attitude / Aptitude / Altitude
- P I V O T

Organizational Culture

Organizational culture is a system of shared assumptions, values, and beliefs, which governs how people behave in organizations. These shared values have a strong influence on the people in the **organization** and dictate how they dress, act, and perform their jobs.

What Role Do You Play

Attitude / Aptitude / Altitude

Attitude - a settled way of thinking or feeling about someone or something, typically one that is reflected in a person's behavior.

Aptitude - capability; ability; innate or acquired capacity for something; talent.

P - Passion

I - Innovation

V - Versatility

O - Openness

T - Tenacity

Strong and barely controllable emotion.

"This defines entrepreneur and entrepreneurship - the entrepreneur always searches for change, responds to it, and exploits it as an opportunity." **Peter Drucker**

Ability to adapt or be adapted to many different functions or activities.

Lack of restriction; accessibility.

The quality or fact of being very determined and continuing to exist.

Joe Harford, MS, CIPP, CSDS
Founder and President
joseph@reclamere.com
814-684-5505 x101

Insider Threats:

Challenges and Mitigation Approaches

James Joshi

Professor, Director of LERSAIS

School of Computing and Information,

University of Pittsburgh

SEI-CERT: definition of Insider Threat

- "a current or former employee, contractor, or business partner who meets the following criteria:
  - has or had authorized access to an organization's network, system, or data
  - has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems"
  - has no malicious intent associated with his or her action (or inaction) that cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems."

Insider threat: agents/actors or influences

- Employees
  - Current and terminated
  - Remote employees
- Partners
  - Contractors/Sub-contractors
  - Outsourced companies
  - Third party Vendors
- Outside collaborations -> collusions
- Mergers and acquisitions
- ….

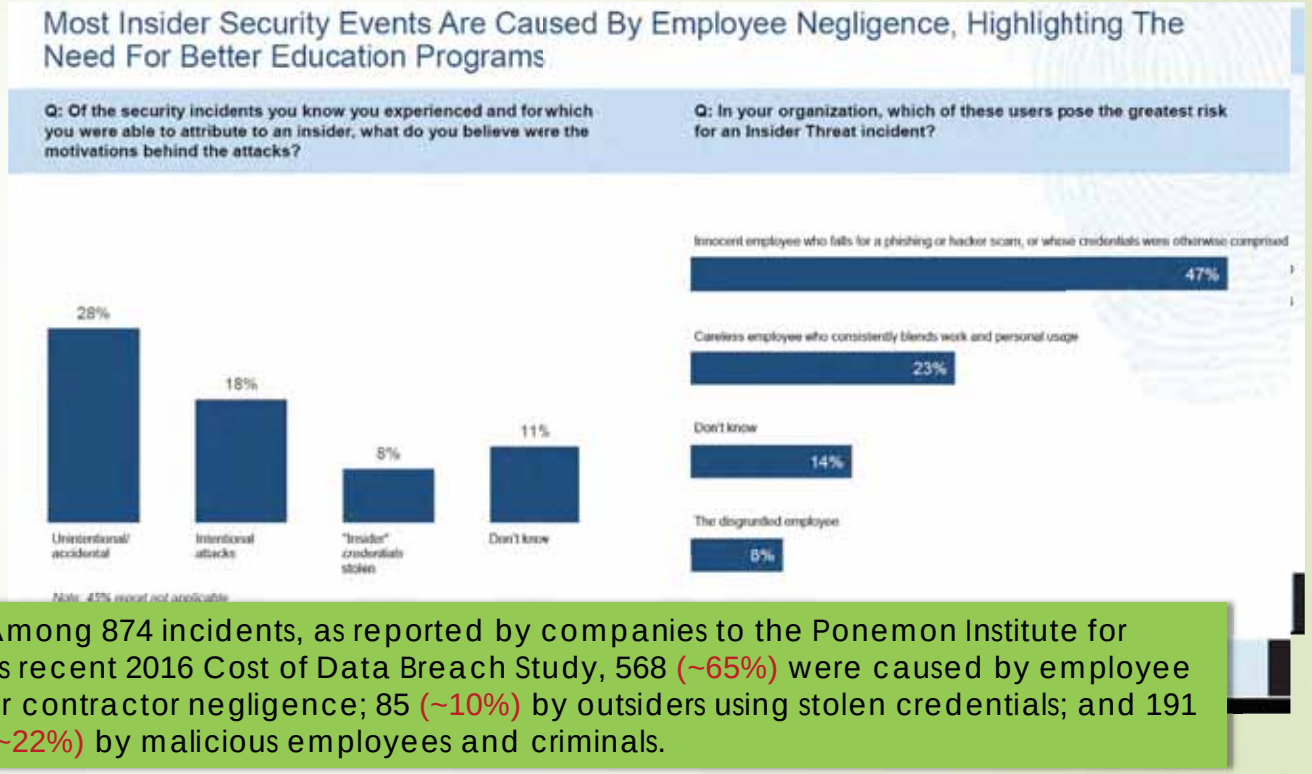
- Exploitation of an opportunity
- Revenge by disgruntled
- Political or social statement
- For competitors (blackmail/bribery)
- ….

- Compromise network security,
- Breach databases,
- Disable security controls,
- Install malware,
- Exfiltrate data,
- Aid adversarial multi-vector information warfare and
- Waste critical resources
- ……

humans remain the weakest link in an organization's cybersecurity

Insider Threat types

- Malicious
  - Sabotage,
  - IP Theft,
  - Espionage,
  - Fraud (financial gain)
- Non-Malicious
  - Negligent users
    - intentionally neglect
    - Misguided activities
  - Untentionanal
    - Human error,
    - Bad judgement,
    - Phishing,
    - Malware
    - Stolen Credentials



Among 874 incidents, as reported by companies to the Ponemon Institute for its recent 2016 Cost of Data Breach Study, 568 (~65%) were caused by employee or contractor negligence; 85 (~10%) by outsiders using stolen credentials; and 191 (~22%) by malicious employees and criminals.

Source: 2017 US State of Cybercrime Survey, conducted by CSO, US Secret Service, Carnegie Mellon University CERT, and Forcepoint.

Some more data ...

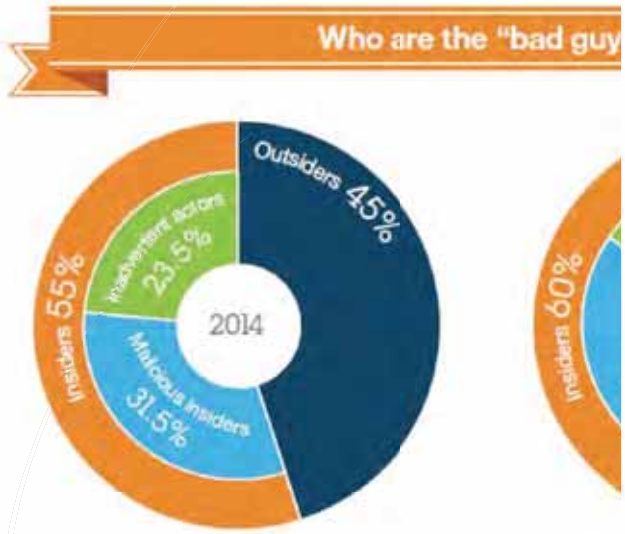


Figure 4. In 2015, outsiders were found to be responsible f
recorded, while 60 percent of attacks were carried out by
organizations' systems.

Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

Fewer

More

58%

71%

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

Example insider attacks

"The year 2013 may be the year of the insider threat. … These incidents highlight the need to improve the ability of organizations to detect, deter, and respond to insider threats".

Edward Snowden – Computer Emergency Response Team (CERT), January 2014.

- NSA & WikiLeaks
- Target Breach in 2013
  - Estimated $1B
- Sony hack in 2014
  - North Korea or Disgruntled Insider? Stolen credentials? Phishing emails?
- Stuxnet – through infected USBs … exploitation of insiders
  - contractors to reach the target (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/)
- 2011 - Wastewater utility in Mesa, AZ (mannal shut-down of OS)
- 2000, a contract employee - disgruntled – in Australian wastewater services company, attacked the facility's supervisory control and data acquisition (SCADA) systems
  - disabled system functions and allowed a total of 800,000 liters of untreated sewage to spill into receiving waters over a period of several weeks.

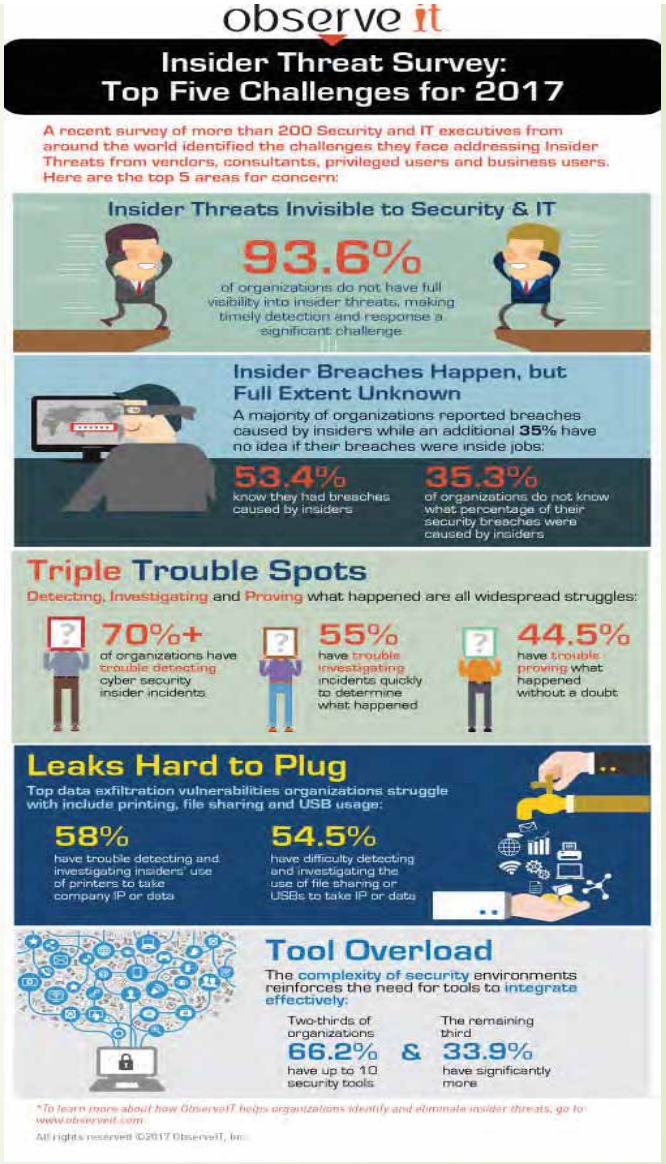
Source: https://www.esecurityplanet.com/network-security/researchers-say-sony-hack-was-insider-breach.html

https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/

Challenges

"Insider threats are influenced by a combination of technical, behavioral, and organizational issues and must be addressed by policies, procedures, and technologies"

"humans remain the strongest and the weakest link in every organization's cybersecurity"



Invisibility

Coverage

DIP

Exfiltration control

Overlaod

Expanding threat environment

- The WEF 2017 Global Risks Report : “cyberattacks, software glitches, and other factors could spark systemic failures that “cascade across networks and affect society in unanticipated ways.”

Source: Key findings from The Global State of Information Security® Survey 2018

- Current and emerging ..
  - Mobile technologies
  - Social Networks
  - Internet of Things
  - Cloud computing
  - Big data
  - ...

Increasing:
- Complexity
- Connectivity
- Pervasiveness

& Constantly
- Evolving

Mitigation Approaches

- Some key issues
  - Human issue is central !!
    - Behavioral monitoring vs. Privacy
  - Existing approaches are typically REACTIVE
  - Can we predict?

Insider attacks are typically preceded by technical and psychological precursors

Mitigation Approaches

- Design & Implement appropriate security programs
  - Procedures and policies
  - Risk Management
  - Security education, training and awareness program (SETA)
- Design Adequate Access Control policies and solutions
- Predict attack: Monitoring and anomaly detection
  - Detect undesirable changes in behavior and tune up security controls

Technical & Psychological precursors

- Download and use of hacker tools
- Access to other users' or customer data (misuse)
- Setup or use of backdoors
- Transmitting large files
- Etc.

- Disgruntlement
- Bad attitude
- Lack of dependability
- Absenteeism
- Etc.

[Greitzer et. al]

Access Control System

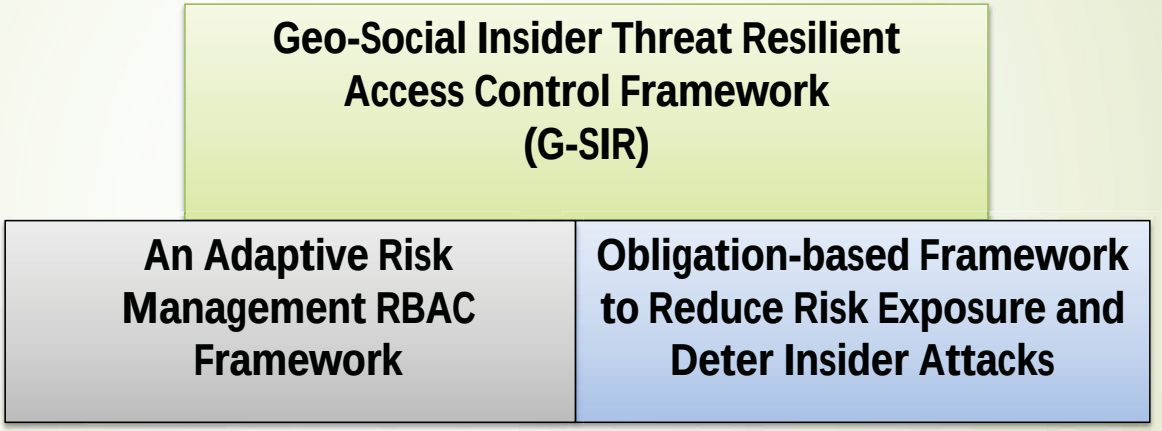
- This is a MUST!
- Restrict the access enforcing
  - Separation of duty
  - Least privilege enforcement

- Challenge: Employees need the privileges, but we need to prevent the abuse those permissions

Current Access Control Approaches

- Access control systems are highly static
  - As long as users have the required credentials, they can access the system
  - What about their behavior?
- Require manual verification and input
  - Manual verification of alerts
  - Input of psychological precursors is slow and subjective

Our proposed adaptive access control approach



Nathalie Baracaldo, "Tackling Insider Threats Using Risk-and-Trust Aware Access Control Approaches". 2016. **PhD Thesis**. *University of Pittsburgh.*

Joint work

Nathalie Baracaldo, Balaji Palanisamy, James Joshi. "G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework," *IEEE Transactions on Dependable and Secure Computing*, IEEE, 2017

Nathalie Baracaldo, James Joshi "An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats" *Computers & Security*. 2013.(Journal)[

Nathalie Baracaldo, James Joshi "Beyond Accountability: Using Obligations to Reduce Risk Exposure and Deter Insider Attacks" *ACM Symposium on Access Control Models and Technologies (SACMAT)*, Amsterdam, The Netherlands. 2013.

Nathalie Baracaldo, James Joshi "A Trust-and-Risk Aware RBAC Framework: Tackling Suspicious Changes in User's Behavior" *ACM Symposium on Access Control Models and Technologies (SACMAT)*, Newark, USA. 2012.

1. An Adaptive Risk Management RBAC Framework

We identify an opportunity to control risk frequently (for each access request) and automatically ☺

- Two concepts:
  - Trust: expectation of future behavior based on the history
  - Risk: likelihood of a hazardous situation and its consequences if it occurs
- We include risk and trust in access control systems to adapt to anomalous and suspicious changes in users' behavior

Requirements

1. Enforce separation of duties (SoD) and cardinality constraints
2. Detect suspicious activities, and establish a trust level for each user
   - Different trust values for users depending on the *context*
3. Different permissions may have different risks associated with them
   - Adapt to suspicious changes in behavior of users by restricting permissions depending on risk values
4. Risk exposure should be automatically reduced, minimizing the impact of possible attacks

In a nutshell…

role

permission

trust_threshold(role)

authorized(*u*,role) & trust(u,c)≥trust_threshold(role)

Trust value of users

- Each user u is assigned a trust value:
  - $0 \leq trust(u,c) \leq 1$ → reflects his behavior
  - Where *c* is the context, and *u* is the user
- Some works exist to calculate this value

Assigning risk to permissions

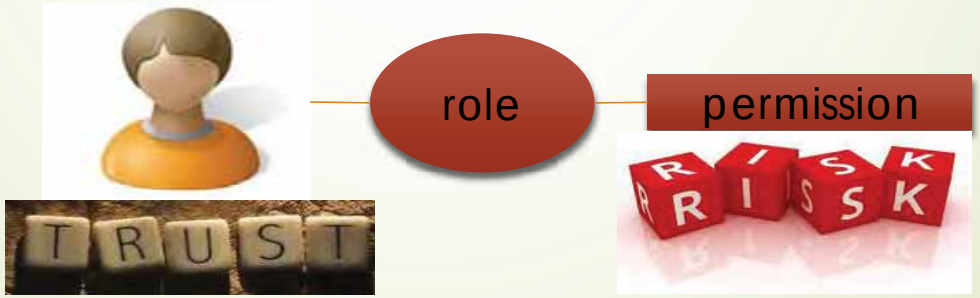
- Each permission is assigned a risk value according to:
  - The *context*
  - The likelihood of misuse
  - The cost of misuse

DEFINITION 1. *The risk of permission* $p = \langle obj, act \rangle \in P$ *in context* $c \in C$, *written as* $rs(p, c)$, *is defined as follows:*

$$rs(p, c) = \sum_{x_p \in MaliciousUsage} Pr[x_p |\ c\ ] * \mathcal{C}(x_p)$$

Risk of roles

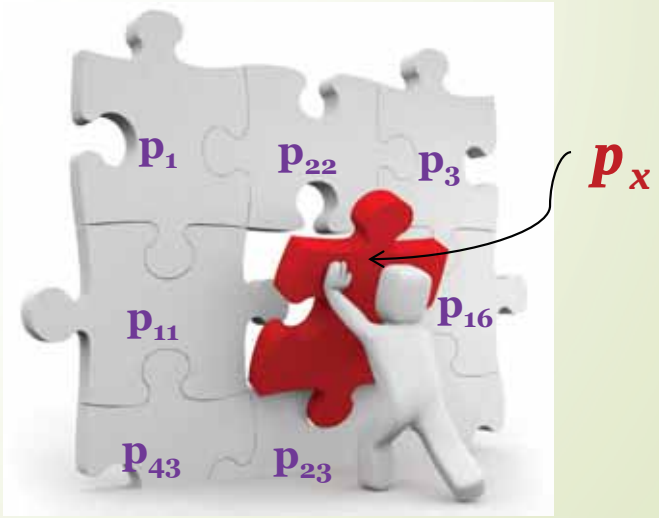
- The risk of activating a set of roles depends on:
  - Context
  - The user that is going to activate the roles
  - Authorized permissions & their risk
  - Inference risk



Inference risk

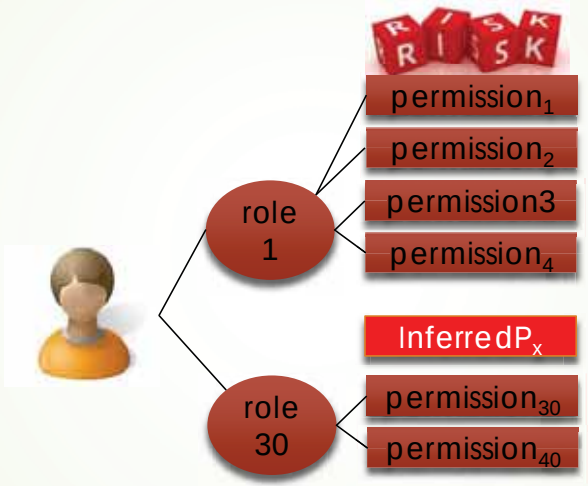
- *Inference Threat:* exists when a user is able to infer unauthorized sensitive information through what seems to be innocuous data he is authorized for
- *Inference tuple:* <*PS*, p_x>

  Shows the minimum information needed (*PS*) to infer p_x



Risk of roles

- Risk exposure of activating a set of roles

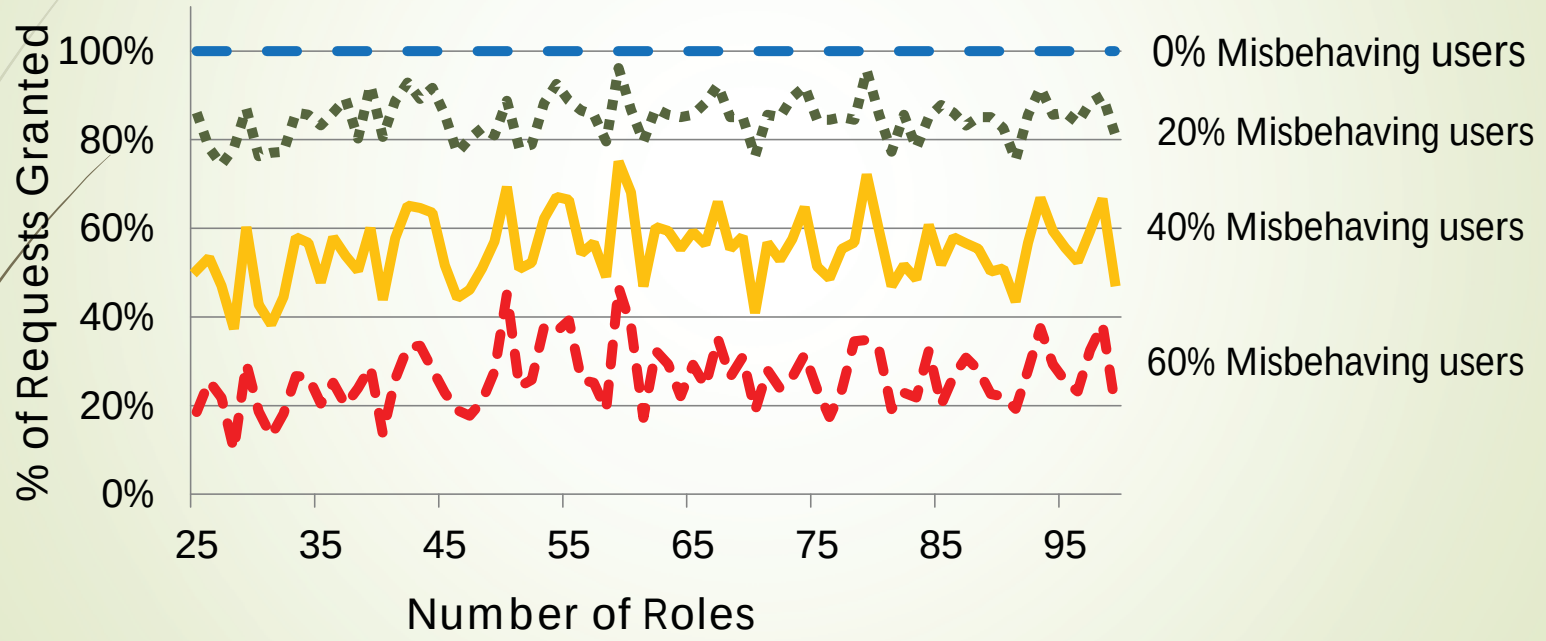


- For a set of roles *RS*, the trust threshold is the normalized version of their risk
- $0 \leq trust\_threshold(RS, c, u) \leq 1$

Experimental Setup

- We generated synthetic *well-formed policies*
- Each point represents the average time of running the algorithm for 30 different policies
- We evaluated our algorithm under two different heuristics for several types of policies

Granted requests for different percentage of misbehaving users



Critical accesses are denied preventing possible attacks

2: Obligation-based Framework To Reduce Risk Exposure And Deter Insider Attacks

- Many application domains require the inclusion of obligations as part of their access control policies

Managing *a posteriori* obligations is challenging

- Once you grant access to a user, there is no guarantee that he will fulfill the associated obligation
- Statistics show that it is not wise to trust users blindly!

Ideally

But this may happen

Especially because

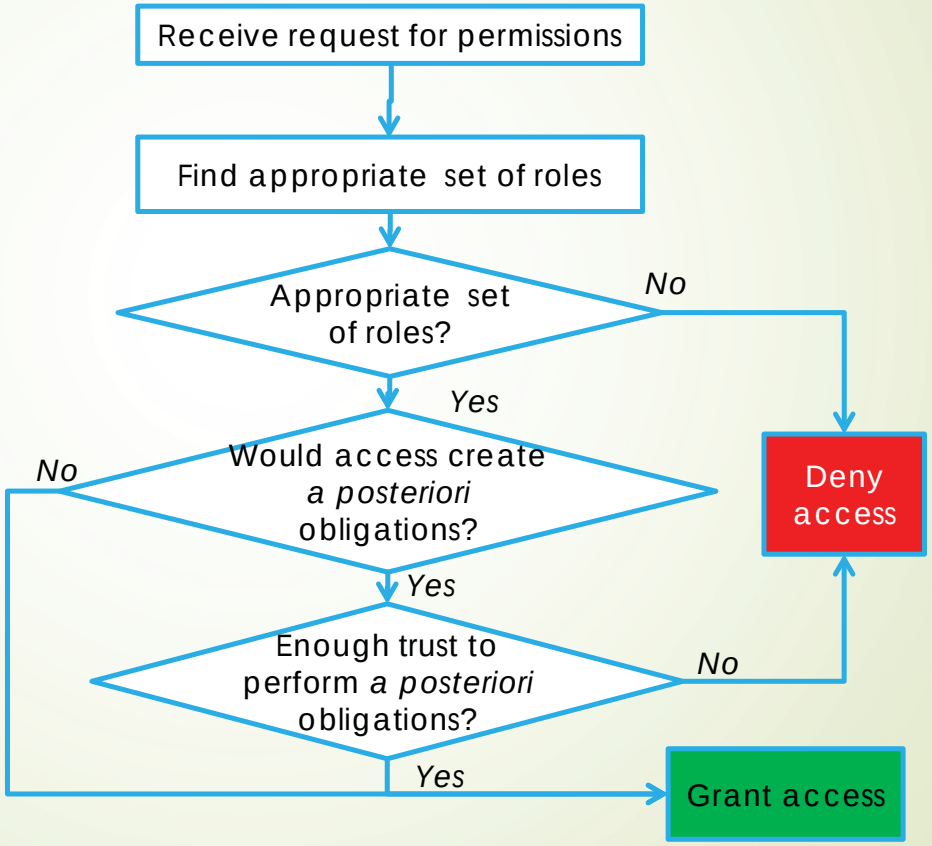
- Every time an *a posteriori* obligation is assigned to a user, there is some risk of non-fulfillment
- The risk exposure depends on the impact of not fulfilling the obligation
  - Delays on the operation
  - Fines
  - Loss of good will
  - Lawsuits

Requirements

- Reduce the risk exposure caused by *a posteriori obligations*
- Identify the trust value of a user based on the pattern of fulfillment of *a posteriori* obligations
- Identify policy misconfigurations
- Identify when a user is likely to become an insider attacker, without invading users' privacy

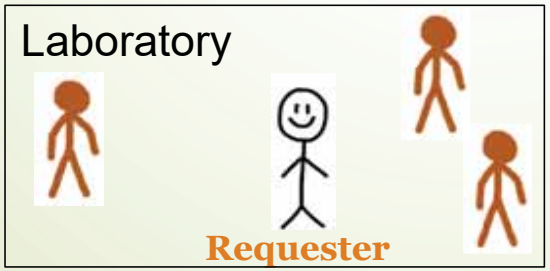
System Overview

- We use standard RBAC
- However, this trust approach can be used for any other access control model that includes obligations



3. G-SIR: An Insider Attack Resilient Geo-Social Access Control System

- Use location and social context to determine access
- Social graph(s)
  - Is a user part of community *X*?
  - Are two users friends?
  - What is their relationship?
  - Are they connected?



Requirements

- Classify users in the vicinity
- Design policy constraints to capture and prevent undesirable geo-social behavior: geo-social contracts, geo-social obligations and trace-based constraints
- Mitigate the risk of colluding users
- Adapt access control decisions to negative changes in behavior of users

Conclusion

- Insider threats are real and difficult to address
- Current solutions are reactive – more proactive solutions are needed
- Mitigation requires technological, policy and organization approaches
  - Significant issues related to negligence or careless users
  - SETA
- Technological and psychological percursor need to be captured
  - Adaptive security approaches can help

CYBERSPACE WORKFORCE SKILLS IN THE U.S. ARMY RESERVE AND ARMY NATIONAL GUARD

Isaac R. Porche, Ph.D.
October 25, 2017

https://www.rand.org/pubs/research_reports/RR1490.html

Photo by Capt. [illegible] Key/U.S. Army

Additional Contributions to the Project Provided By:

- Caolionn O'Connell and Tina Panis - CEI Database Analysis
- John S. Davis, II - NSA Cyber Tasks Analysis
- Bradley Wilson - LinkedIn Analysis on Cyber Skills
- Chad C. Serena - Role of the Reserves
- Tracy C. McCausland and Susan Strauss - Survey and HSPC
- Erin-Elizabeth Johnson - Communications Analyst
- Brian D. Wisniewski - Role of the Reserves
- Michael Vasseur - CISCO Analysis
- Kristin Van Able - Visualization of Survey Response
- Pete Schirmer - Project Concepts
- Management - Mike Hansen, Brian Hallmark, Shanthi Nataraj, Michael Linick

What does the Army Cyberspace Workforce do?

REFERENCE(S): 1.

Bottom Line Up Front

- Objective:
  - The Army asked the Arroyo Center to inventory the cyber skills resident in the reserve component
- Method:
  - The cornerstone of the study is analysis of data from the Civilian Employment Inventory (CEI) database
- Conclusions:
  - The Army will likely need more personnel with Cyberspace Workforce skills than it has now, both in the Active and Reserve components, based on growing demands
  - Many guard and reserve soldiers work in civilian jobs and have skills the Army needs for its Cyberspace Workforce
  - We estimate that over 100,000 reserve component personnel have some competence in skills relevant to the Cyberspace Workforce
  - Using the extrapolated data, we calculate the untapped potential in the guard and reserve as over 11,000 personnel

Preview of findings, observations, and recommendations

DEMAND

for cyber security personnel continues to grow in all sectors

THE CEI DATABASE

provides useful information toward gauging the number of guard and reserve soldiers with cyber skills

CIVILIAN-TRAINED CYBER EXPERTISE

exists and is used in the guard and reserve; tens of thousands of personnel have some cyber expertise

CONTINUOUS PRACTICE

is required to retain cyber proficiency


GROWTH IN DEMAND
SOLDIER SKILLS
TRAINING AND ASSIGNMENTS
CONCLUSIONS, NEXT STEPS

GROWTH IN DEMAND

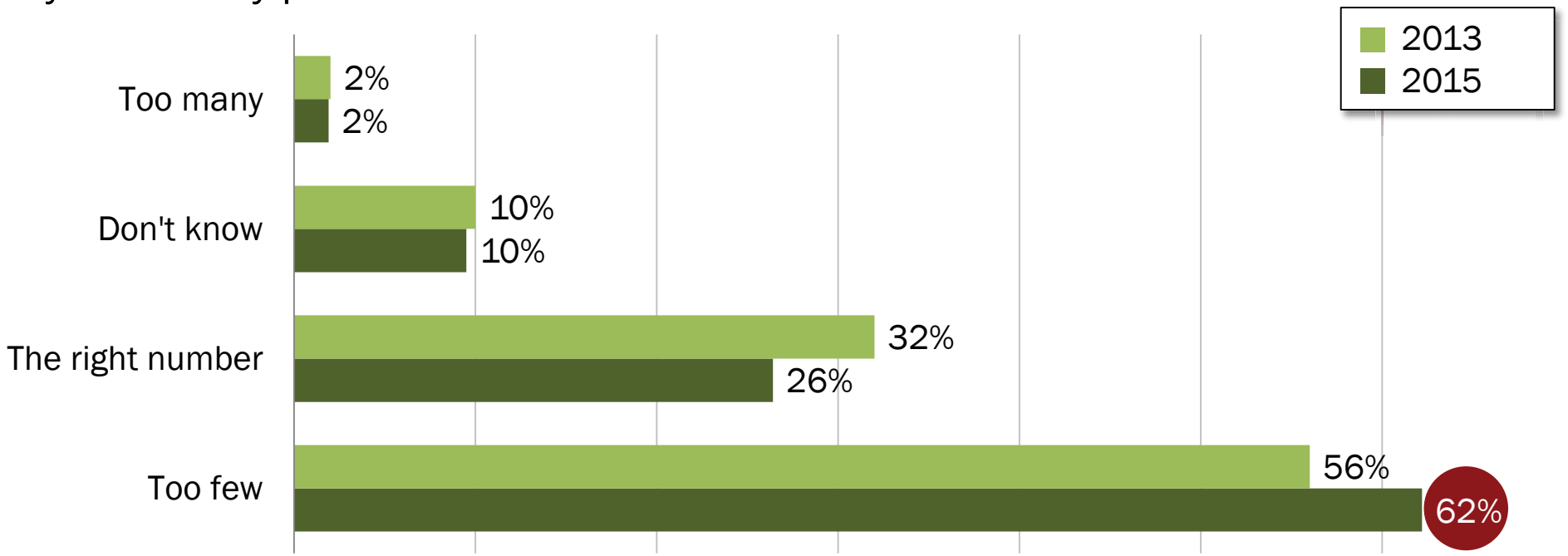
SOLDIER SKILLS

TRAINING AND ASSIGNMENTS

CONCLUSIONS, NEXT STEPS

Multiple studies indicate high demand for cybersecurity personnel among companies in the United States

Q: Does your organization have too many, too few, or the right number of cybersecurity professionals?

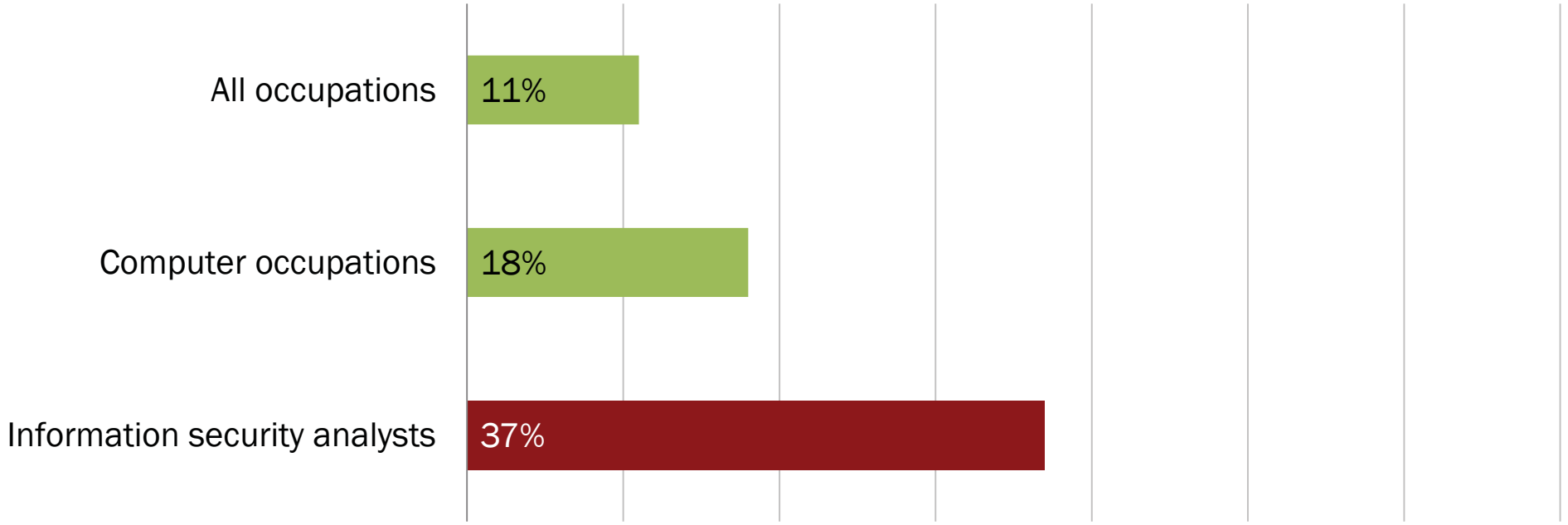


Michael Suby, *The 2013 (ISC)² Global Information Security Workforce Study*, Mountain View, Calif.: Frost & Sullivan, 2013.

Michael Suby and Frank Dickson, *The 2015 (ISC)² Global Information Security Workforce Study*, Mountain View, Calif.: Frost & Sullivan, 2015.

The demand for information security analysts is projected to increase

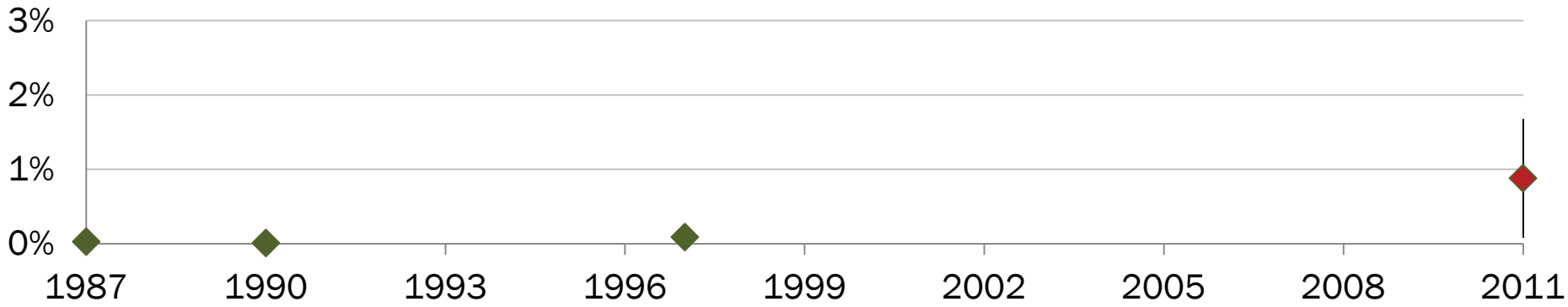
Q: What is the projected demand for information security analysts between 2012 and 2022?



U.S. Bureau of Labor Statistics, "Employment Projections," web site, undated. As of September 3, 2015: http://www.bls.gov/emp/

Information needs vary by sector across U.S. companies, but the overall trend is upward

Q: On average, what percentage of staff are information security personnel?

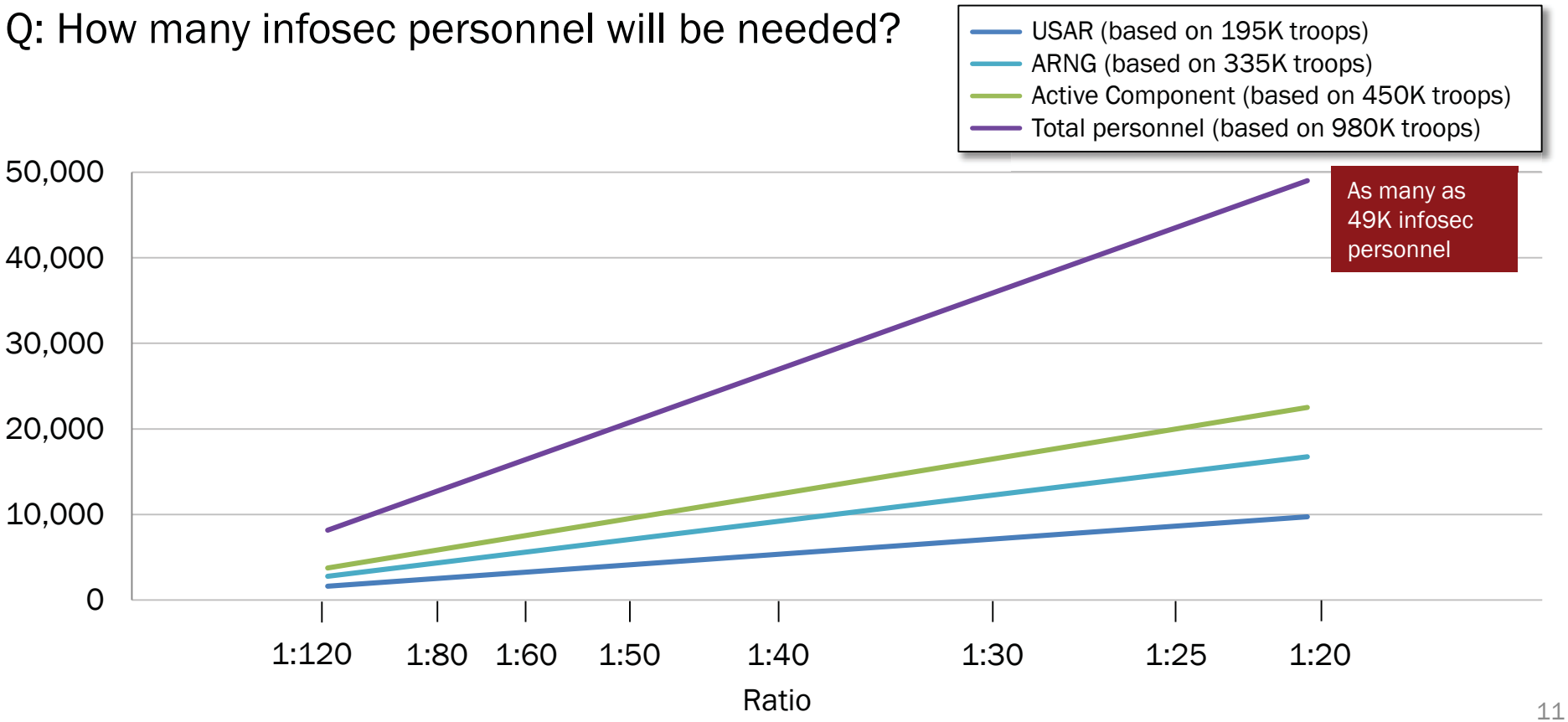


	1987	1990	1997	2011
Low	0.03%	0.01%	0.02%	0.08%
High	0.03%	0.01%	0.16%	1.68%
Average	0.03%	0.01%	0.09%	0.88%

Harold F. Tipton and Micki Krause, Information Security Management Handbook, 6th Edition, Boca Raton, Fl.: Auerbach Publications, 2007.
Lawrence A. Gordon, Martin P. Loen, William Lucyshyn, and Robert Richardson, *CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2006.
Charles Cresson Wood, *Information Security and Data Privacy Staffing Levels: Benchmarking the Information Security Function*, Houston, Tex.: Information Shield, 2012.

Based on 2021 Army end-strength estimates and the acceptable ratios, we calculated the demand for infosec personnel

Q: How many infosec personnel will be needed?



GROWTH IN DEMAND

SOLDIER SKILLS

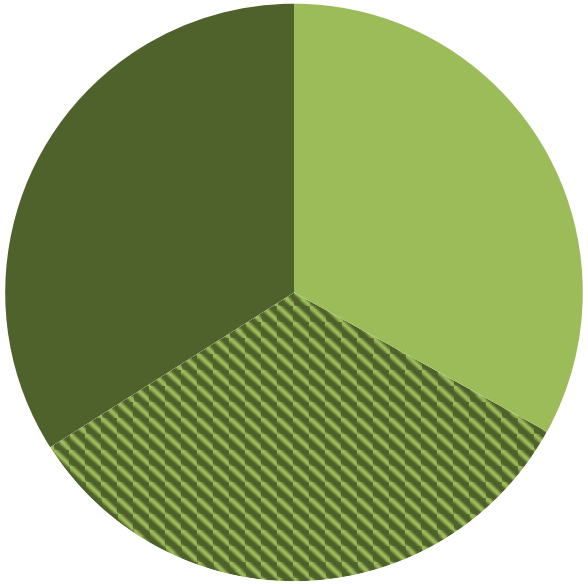
TRAINING AND ASSIGNMENTS

CONCLUSIONS, NEXT STEPS

The guard and reserve may have untapped potential

Q: Where do staff use cyber skills relevant to the Cyberspace Workforce?

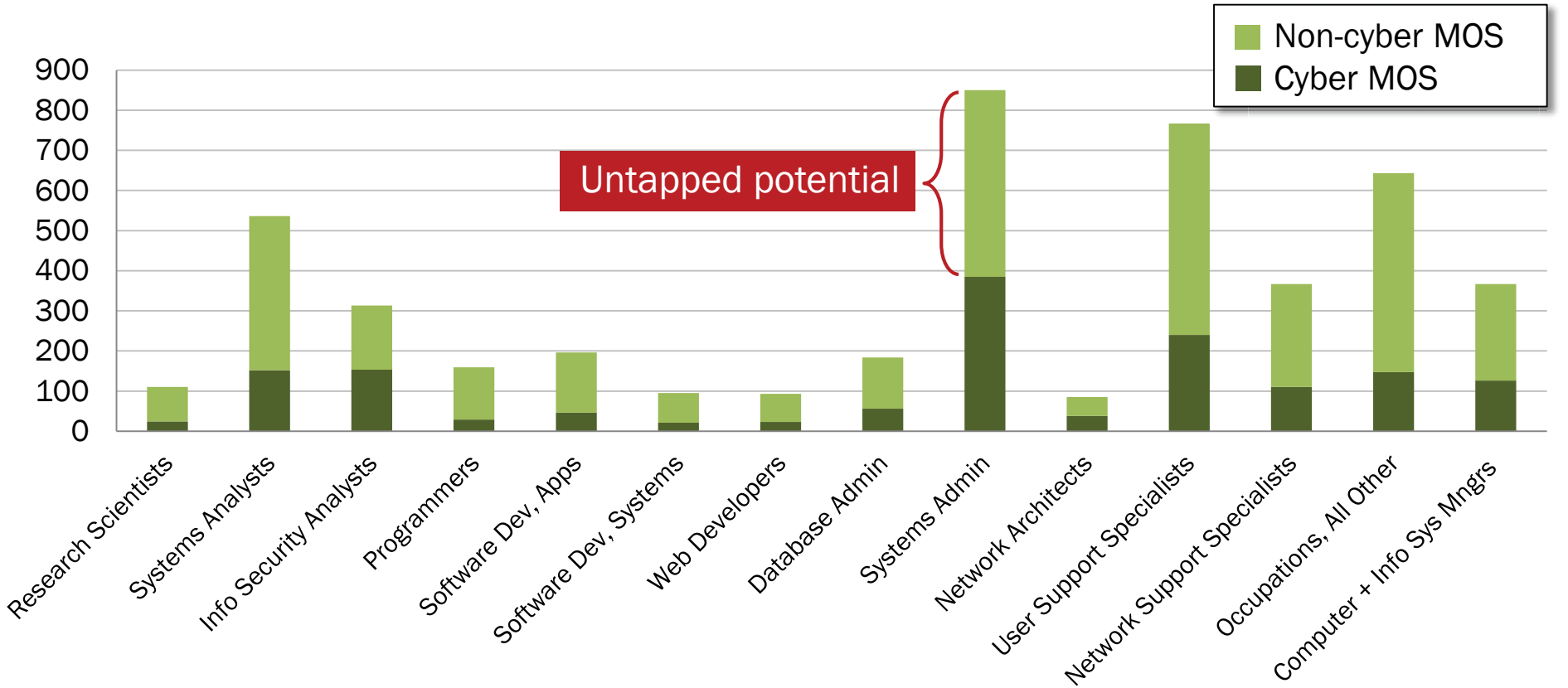
MILITARY ONLY
Possible preparedness issues?



CIVILIAN ONLY
Is this untapped potential?

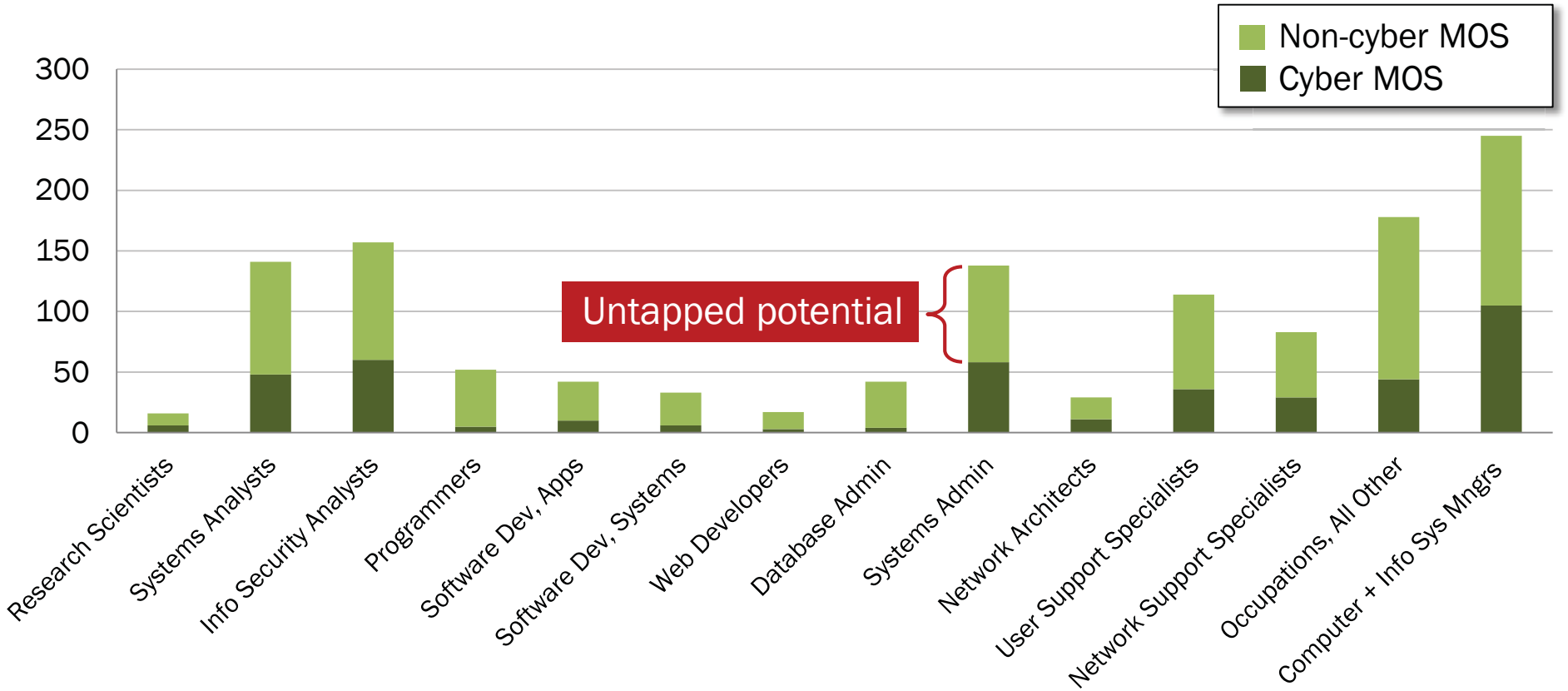
MILITARY AND CIVILIAN
Deep expertise, highly trained

Looking at the number of ARNG civilian professionals by MOS reveals untapped potential



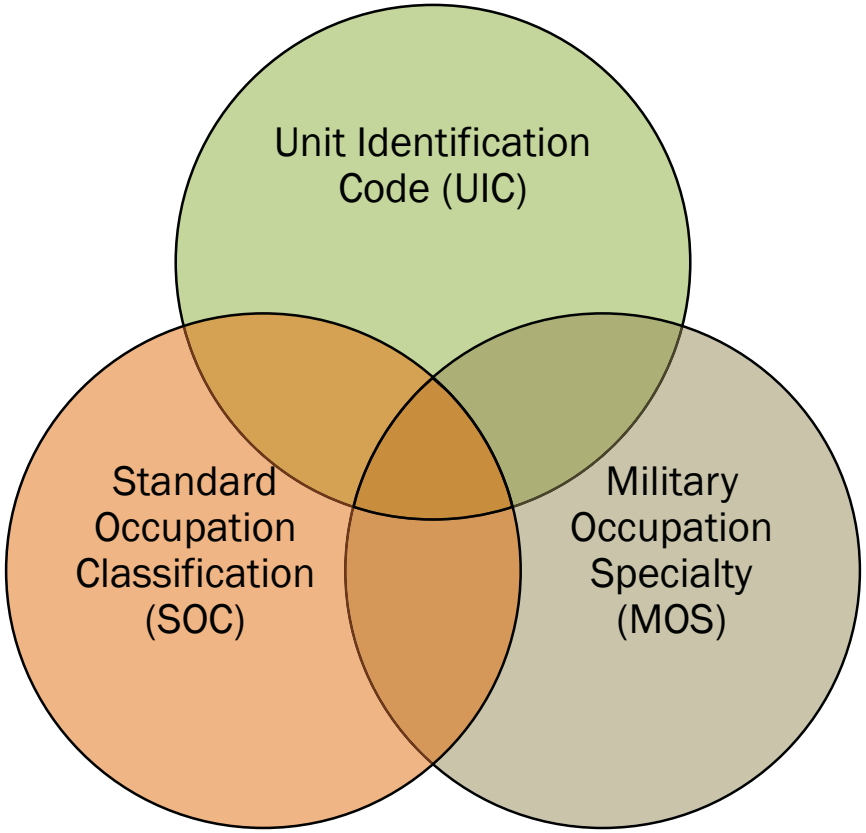
Data analysis from the CEI database

Similarly, looking at the number of USAR civilian professionals by MOS reveals untapped potential

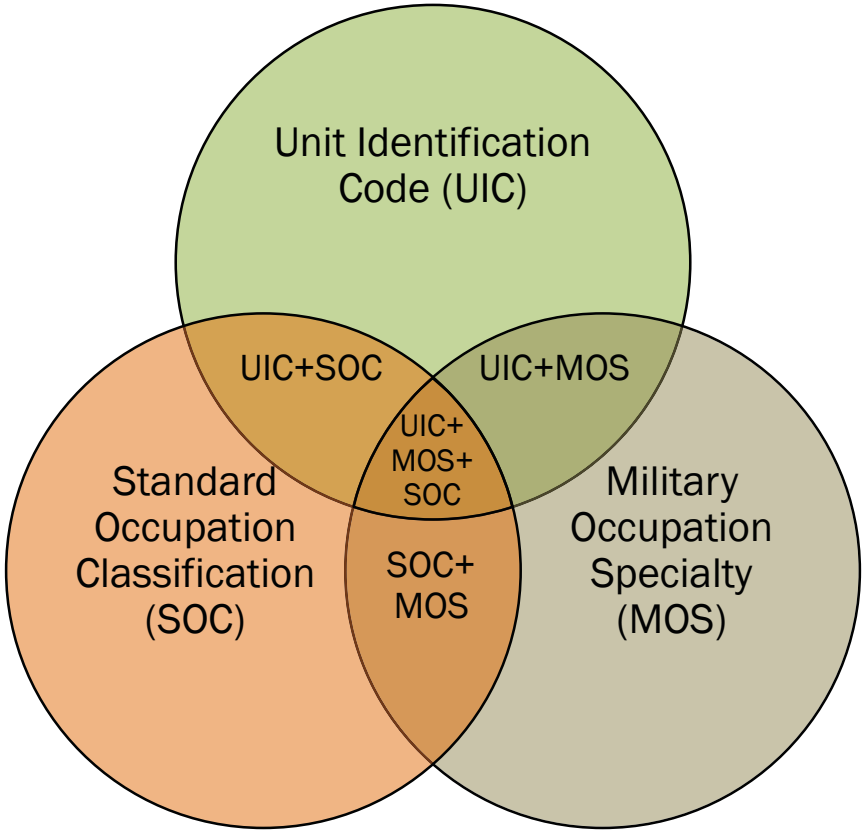


Data analysis from the CEI database

A broader look at identifying cyber expertise



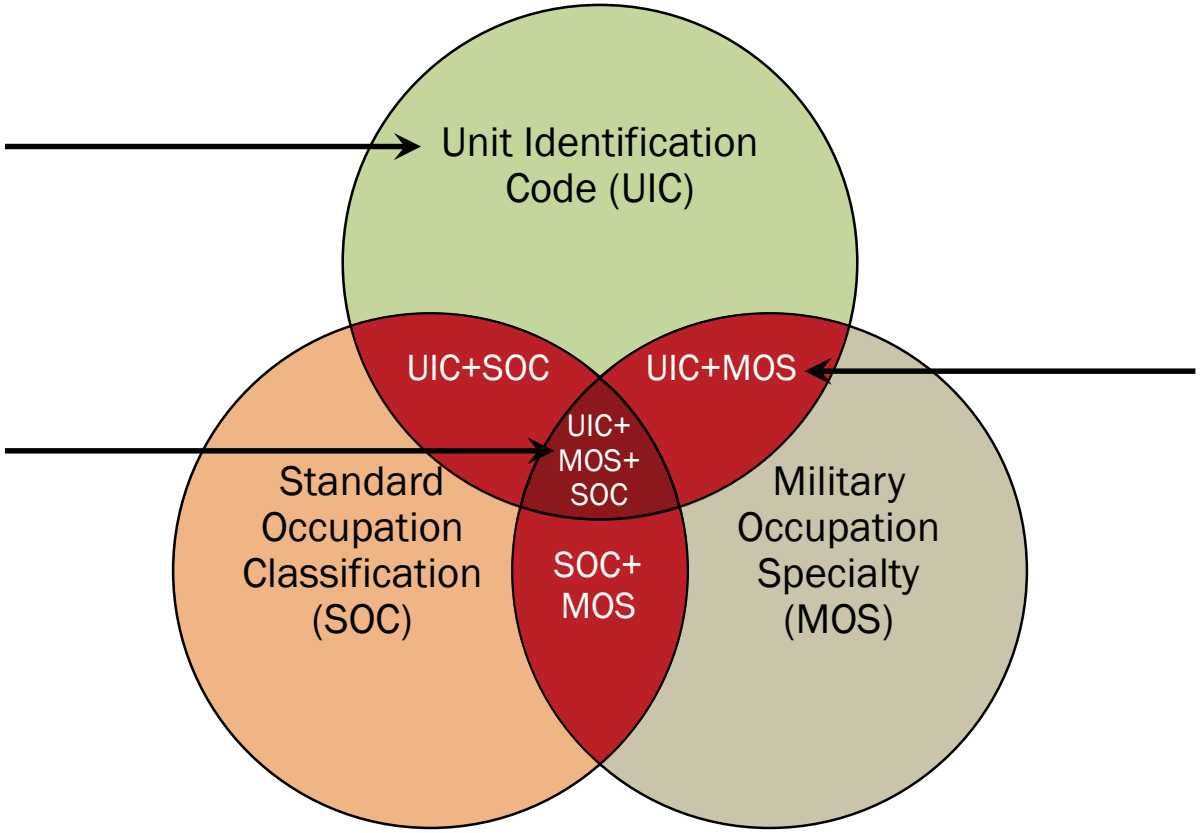
A broader look at identifying cyber expertise



Level of cyberspace operations expertise, by wedge

Outer wedges:
PARTIAL
cyberspace
operations
expertise

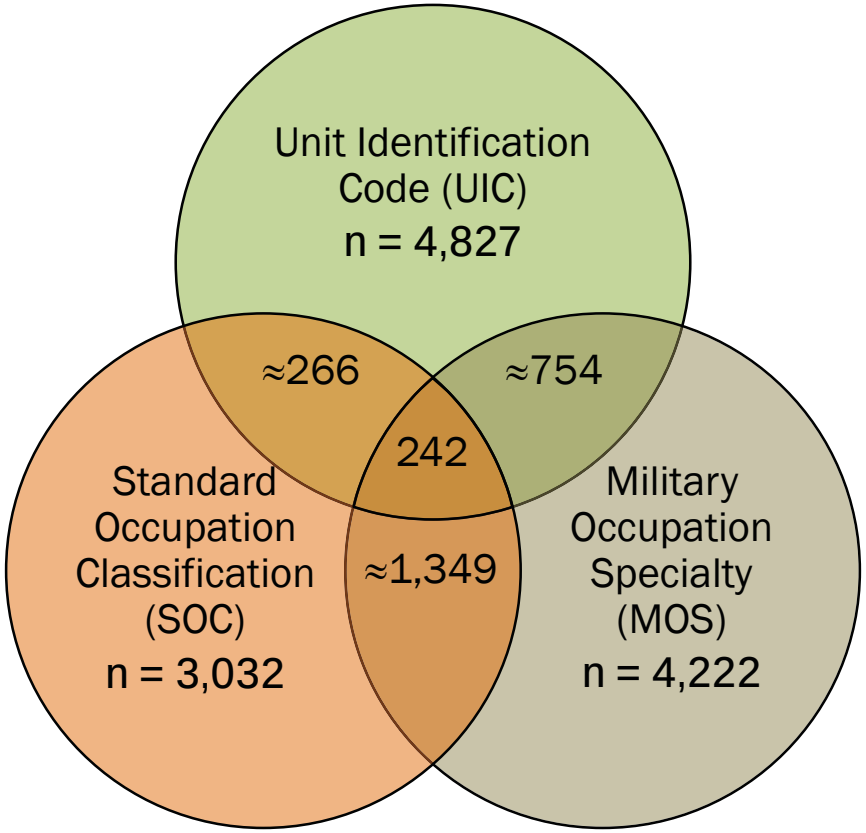
Center wedge:
DEEP
cyberspace
operations
expertise



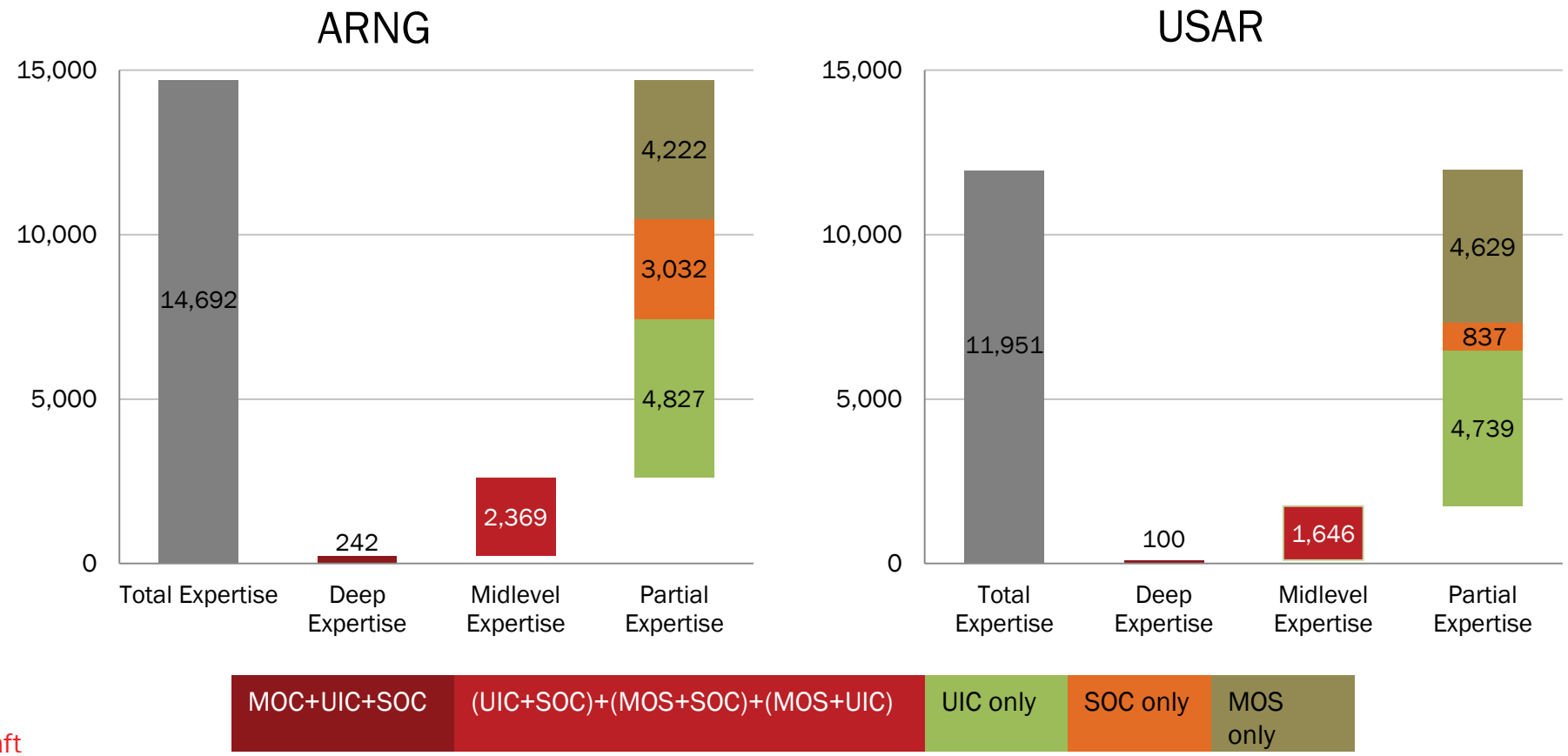
Middle wedges:
MIDLEVEL
cyberspace
operations
expertise

ARNG: Analysis of entries from the CEI database

Is this untapped potential?



At least 32,000 ARNG and USAR personnel have some competence in skills relevant to the Cyberspace Workforce



draft

Extrapolation to the total guard and reserve shows up to an estimated 105,179 personnel have some competence in skills relevant to the Cyberspace Workforce

	CEI Number	Sum of Estimates for ARNG+USAR	
		Lower Bound	Upper Bound
Partial cyber expertise	27,629	86,347	89,169
Midlevel cyber expertise	4,406	14,201	15,541
Deep cyber expertise	259	890	1,251
Any (sum of partial, midlevel, deep)	32,294	102,221	105,179
N (Total)	226,220	550,000	

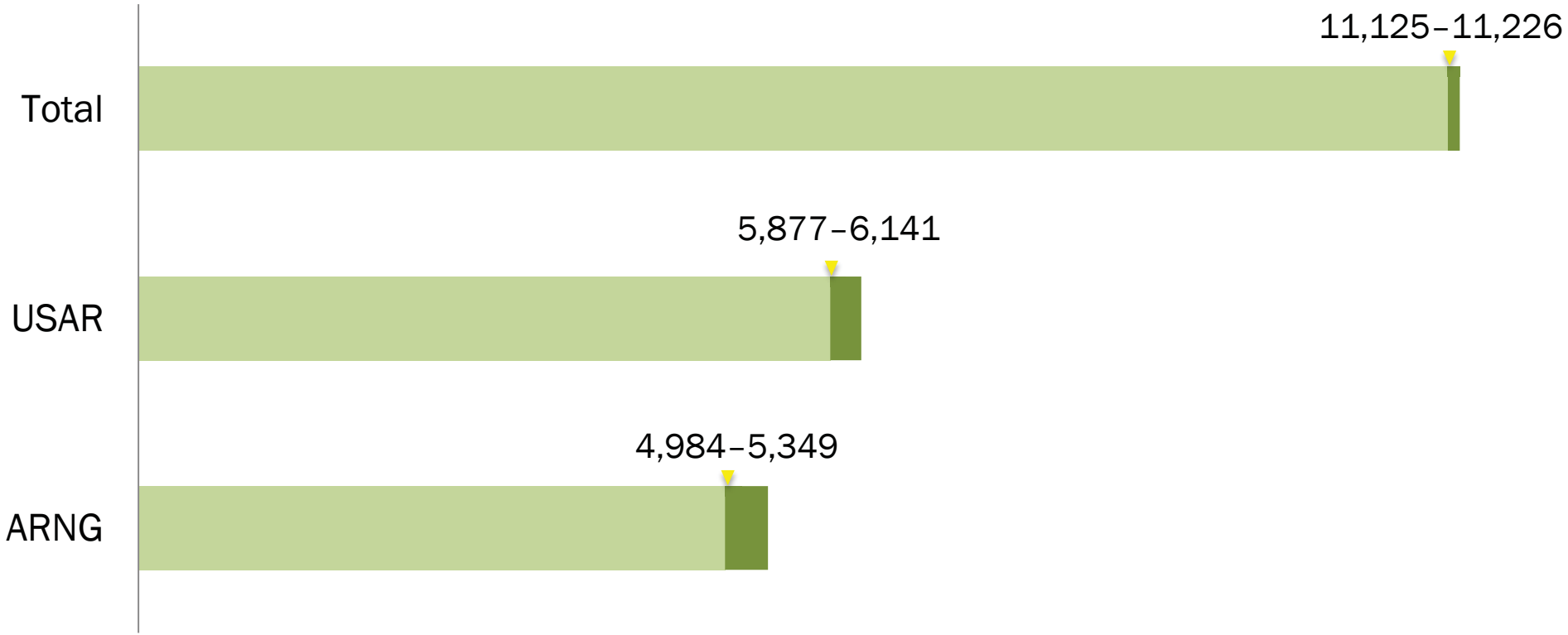
This projected supply represents potential to meet the projected demand for cyber expertise

Q: What is the projected (potential) supply from the RC?

	Low Estimate	High Estimate
Deep expertise	890	1,251
Midlevel expertise	14,201	15,514
Partial expertise	86,347	89,169

Potential future demand for the total Army: 49,000

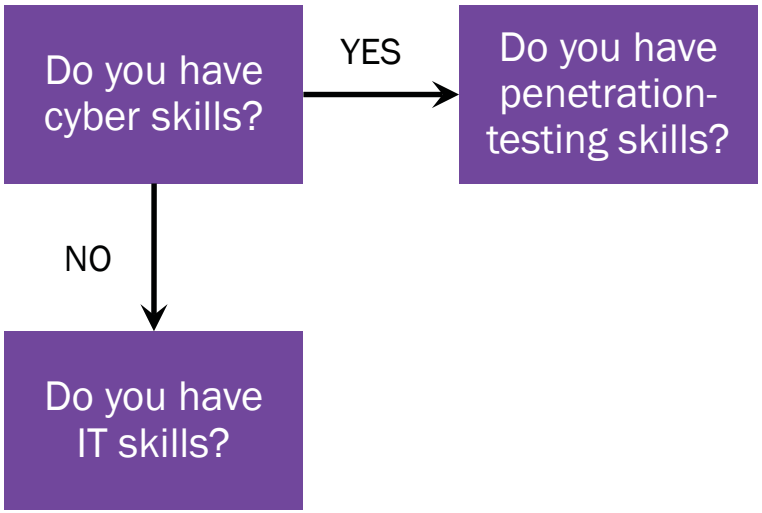
Using the extrapolated data, we calculate the untapped potential in the guard and reserve at as many as 11,226 personnel



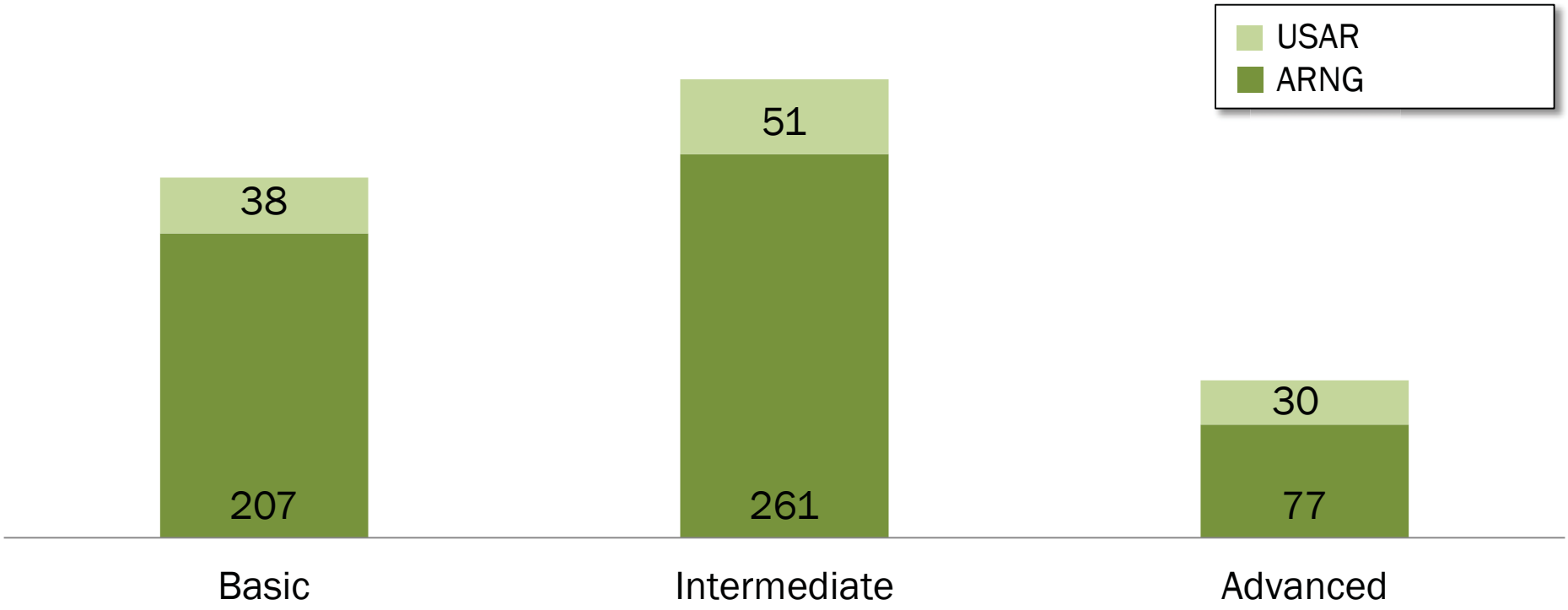
We surveyed select guard and reserve soldiers to identify specific skills that exist in the component

https://www.randsurvey.org/skills/

Sample questions



Respondents indicated varying levels of cyber expertise



NOTE: There were 668 respondents who reported having cyber expertise, but one respondent did not provide a level of expertise.

GROWTH IN DEMAND

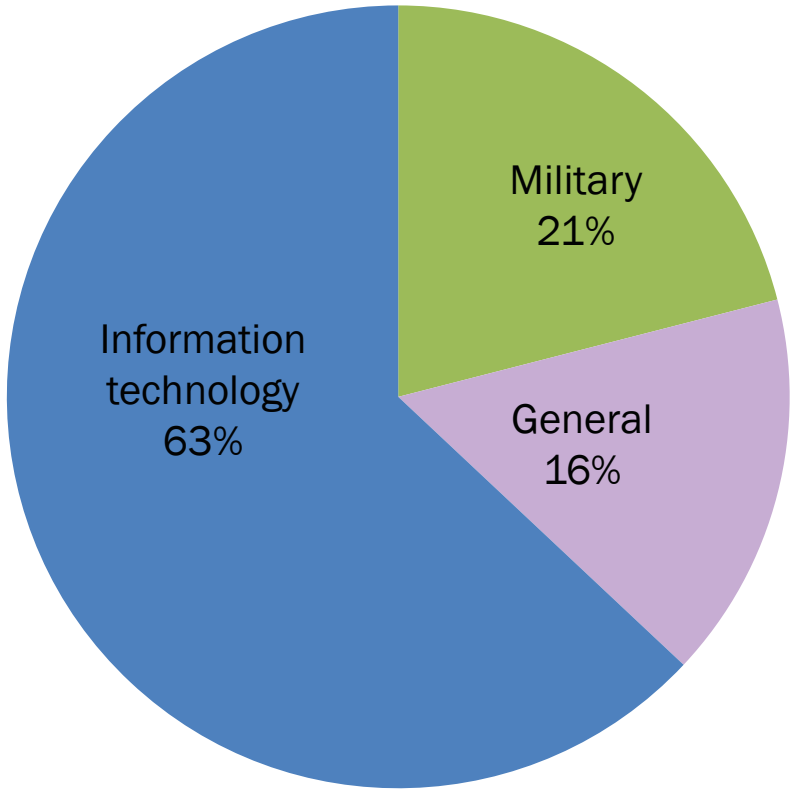
SOLDIER SKILLS

TRAINING AND ASSIGNMENTS

CONCLUSIONS, NEXT STEPS

We found that only one-fifth of all cyber job KSAs are inherently military

- Evaluated the Knowledge, Skills, and Attributes (KSAs) of 26 different cyber job roles (e.g., BDA Analyst, CND Analyst, CND Incident Responder, Cyberspace Policy and Strategy Planner, Data Administrator, Software Engineer, etc.)
- KSAs divided into three categories
  1. Military (e.g., intel confidence levels, Joint Targeting Cycle)
  2. General (e.g., preparing and presenting briefs, analytical thinking, non-specialized software [e.g., MS Word])
  3. Information technology (e.g., virtualization products like VMware, TCP/IP networking protocols, database administration)



What do other organizations do to manage populations with special skills?

Organization Type	Organization(s)	Notes
Foreign military	• UK's Land Information Assurance Group	• Is a cyber reserve unit • Older entrants allowed • All training through civilian employer
U.S. government	• Federal civilian workforce • National Security Agency • Defense Language Force Management*	• Recruitment of students • Outreach to secondary schools and lower
Other	• Medical and Dental Corps* • Judge Advocate General Corps*	• Recruitment of trained graduates of medical and law schools

* Uses Military Accessions Vital to the National Interest (MANVI), which allows noncitizens with in-demand skills to join the Army in exchange for expedited U.S. citizenship.

GROWTH IN DEMAND

SOLDIER SKILLS

TRAINING AND ASSIGNMENTS

CONCLUSIONS, NEXT STEPS

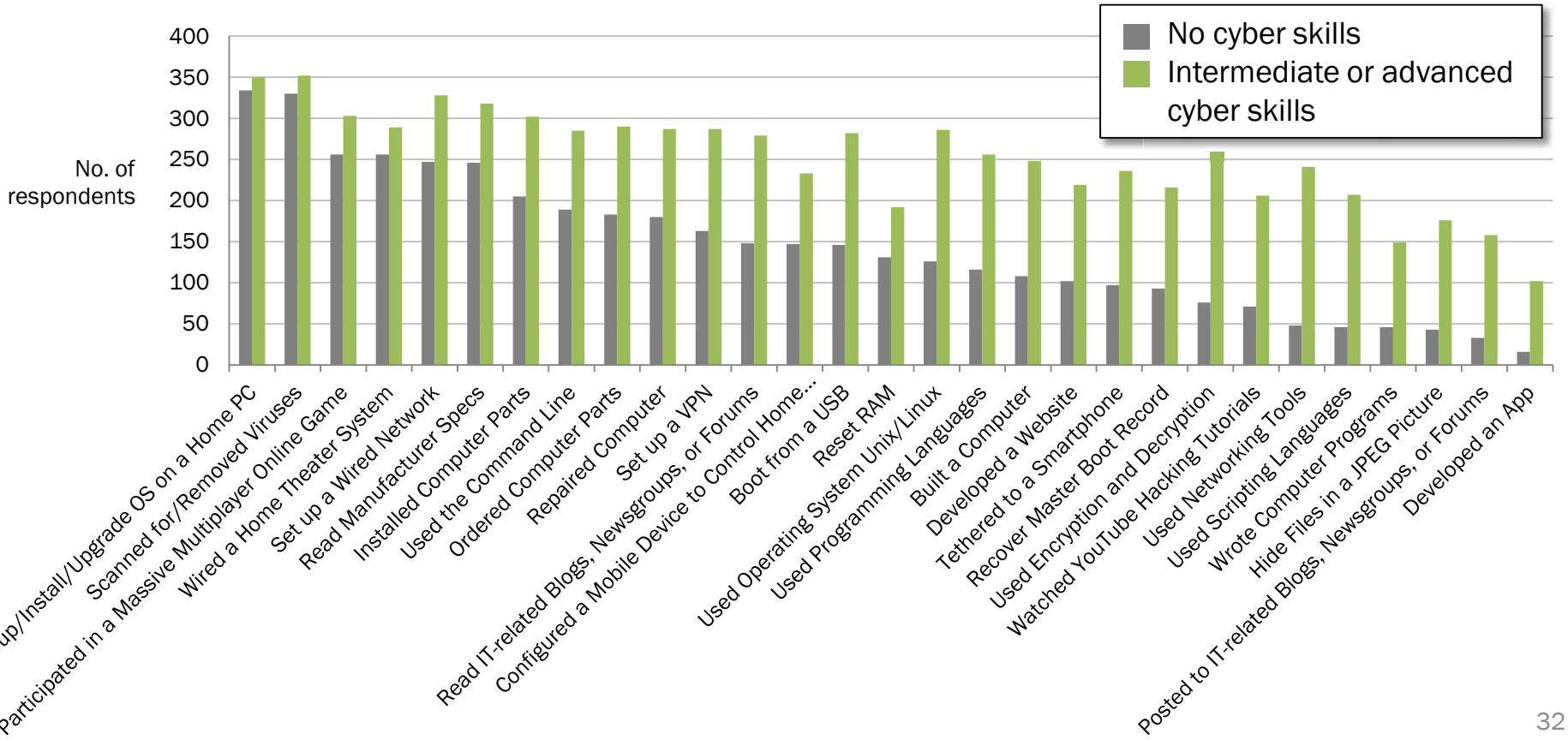
Key findings and observations

- Demand for a cyberspace workforce continues to grow in all sectors
- The CEI database provides useful information towards gauging the number of guard and reserve soldiers with cyber skills
- The guard and reserve use civilian-trained personnel and have tens of thousands of personnel with some cyber expertise
  - The guard and reserve have personnel with skills relevant to the cyberspace workforce, but many are not in specific jobs that use those skills; they represent the untapped potential
  - Those underused personnel are interested in applying their skills to their Army careers
- Generally accepted that proficiency in cyberspace operations requires continuous practice
  - Guard and reserve soldiers who exercise their relevant cyber skills in their day job have an advantage
  - Basic skills to support the CMF can be gained in the civilian sector

Recommendations for incorporating guard and reserve soldiers into the Army's Cyber Workforce

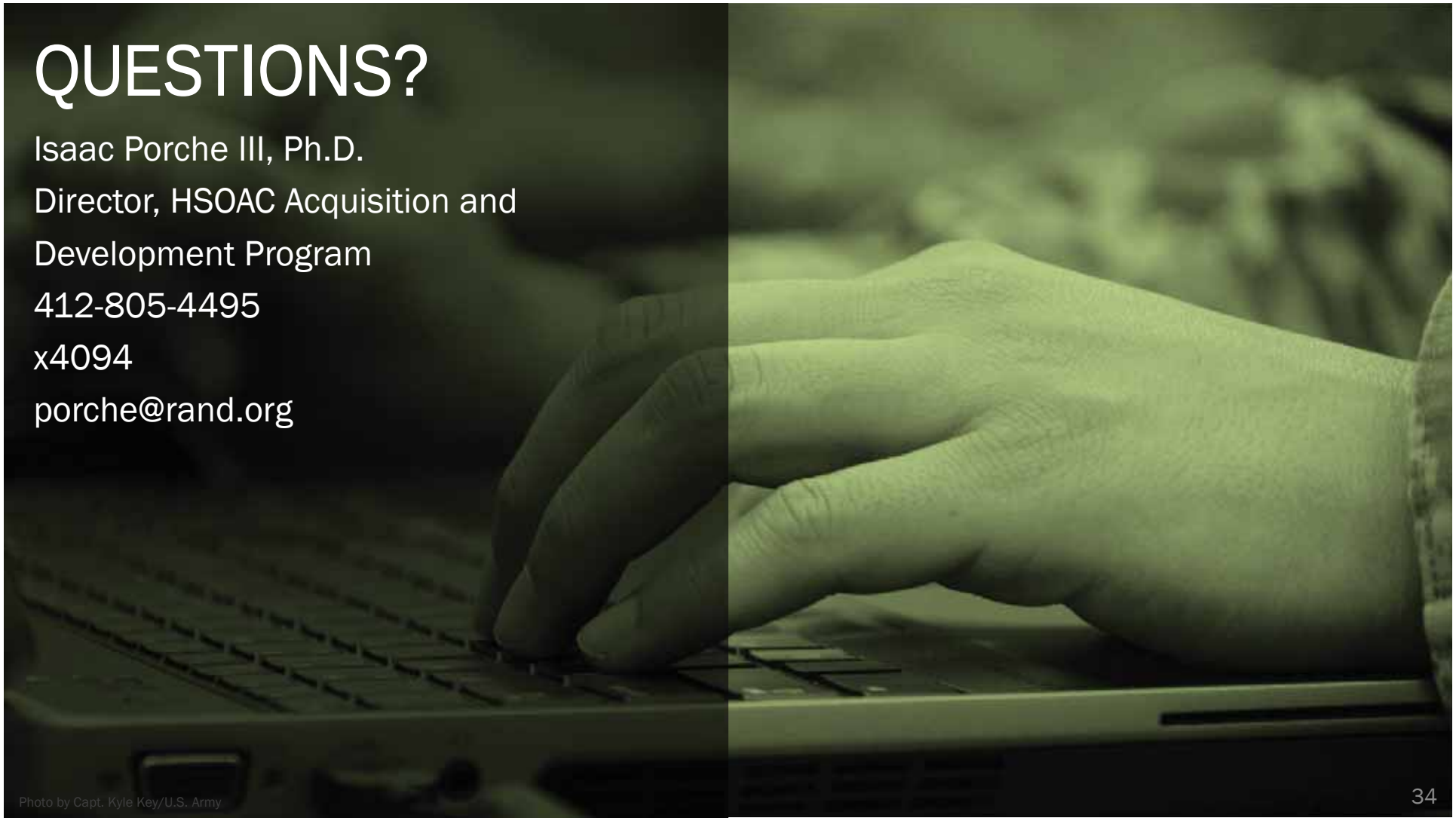
- Continue to tap into the existing "cyber" talent in the ARNG and USAR
  - Take advantage of guard and reserve soldiers who work in civilian jobs requiring cyberspace operations expertise—they could potentially contribute to the Cyber Mission Force and to other organizations
- Explore models from other service/countries for interesting options; for example,
  - The UK LIAG (a cyber reserve unit) allows civilians to join at age 50 and requires entrants to be fully trained by their civilian occupation

Future work: Analyze biodata collected from survey respondents



Current Reserve and National Guard Cybersecurity Work

- Sept. 2017 - The West Virginia Secretary of State's Office and the West Virginia Military Authority engaged in a partnership that will provide members of the WVNG specializing in Cyber Systems Operations to join the daily operations of the West Virginia Secretary of State's Office to assess elections systems and monitor cybersecurity.
- Nov. 2016 - The Ohio Secretary of State's office has engaged with the National Guard's cyberprotection unit to test the state's network to find vulnerabilities and search the state's election system for malicious activity.
- Nov. 2016 - Lt. Gen. Charles Luckey, the Reserve's current chief, recently began a geographic and demographic analysis of home stations. The goal of the study is to determine where the Reserve should be putting their cyber forces in order to "both capture talent and make it more palatable to stay in the Army."



QUESTIONS?

Isaac Porche III, Ph.D.
Director, HSOAC Acquisition and Development Program
412-805-4495
x4094
porche@rand.org

Photo by Capt. Kyle Key/U.S. Army

Other observations from CEI data and survey responses

- Guard and reserve soldiers have a range of skills relevant to the cyberspace workforce, including some advanced skills
  - Most use these skills in the Army, but many do not
  - Those who do not are overwhelmingly interested in doing so
  - They represent untapped potential
- Many cannot use these skills because
  - There are no relevant jobs in their units
  - They are confused about how to pursue a cyber career in the military

References

1. U.S. Department of Defense, *Cyberspace Workforce Management*, DoDD 8140.01, August 11, 2015.
2. Michael Suby, *The 2013 (ISC)^2 Global Information Security Workforce Study,* Mountain View, Calif.: Frost & Sullivan, 2013.
3. Michael Suby and Frank Dickson, *The 2015 (ISC)^2 Global Information Security Workforce Study*, Mountain View, Calif.: Frost & Sullivan, 2015.
4. U.S. Bureau of Labor Statistics, "Employment Projections," web site, undated. As of September 3, 2015: http://www.bls.gov/emp/
5. Harold F. Tipton and Micki Krause, Information Security Management Handbook, 6th Edition, Boca Raton, Fl.: Auerbach Publications, 2007.
6. Lawrence A. Gordon, Martin P. Loen, William Lucyshyn, and Robert Richardson, *CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2006.
7. Charles Cresson Wood, *Information Security and Data Privacy Staffing Levels: Benchmarking the Information Security Function*, Houston, Tex.: Information Shield, 2012.
8. http://www.sos.wv.gov/News-Center/Pages/Cybersecurity-National-Guard.aspx
9. http://www.cnn.com/2016/11/01/politics/election-hacking-cyberattack/index.html
10. https://federalnewsradio.com/on-dod/2016/11/new-army-reserve-chief-asks-whether-reservists-stationed-right-places/

The State of Security Education: Phishing and Beyond

About Wombat Security

- Born from research at Carnegie Mellon University in 2008
- Achieved over 100% year over year growth in sales four years in a row
- Ranked 144 on Deloitte Technology Fast 500™
- A leader for 3 consecutive years in the Gartner Magic Quadrant

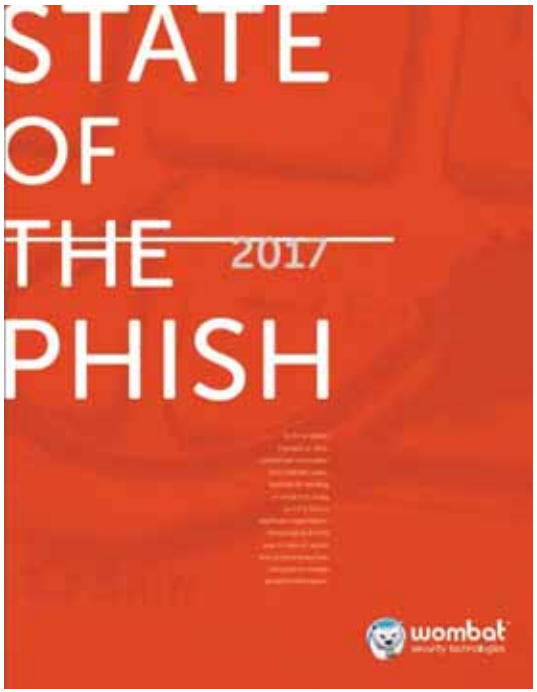
Deloitte. Technology Fast500

Carnegie Mellon

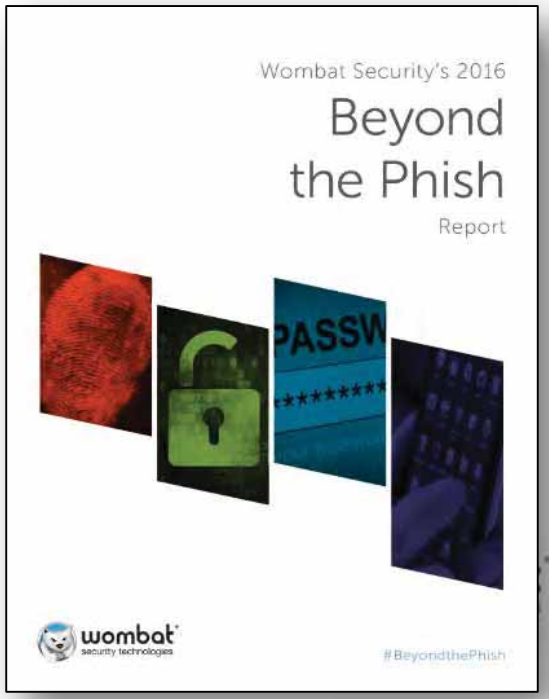
GARTNER'S MAGIC QUADRANT

wombat security technologies

Research



2017 report just released!



User Risk Report 2017

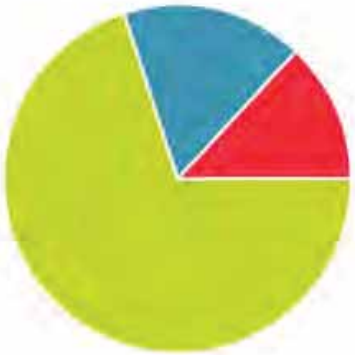
What Do End Users Know?

Phishing

What Is Phishing?

Respondents in the US and the UK had similar levels of understanding of this topic:

GLOBAL AVERAGE



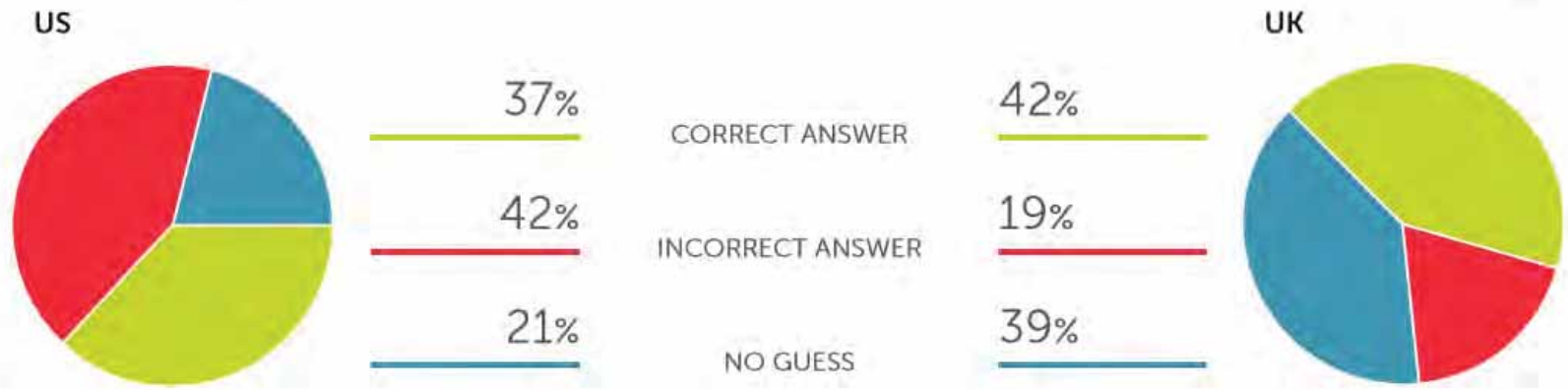
70%
CORRECT ANSWER

17%
INCORRECT ANSWER

13%
NO GUESS

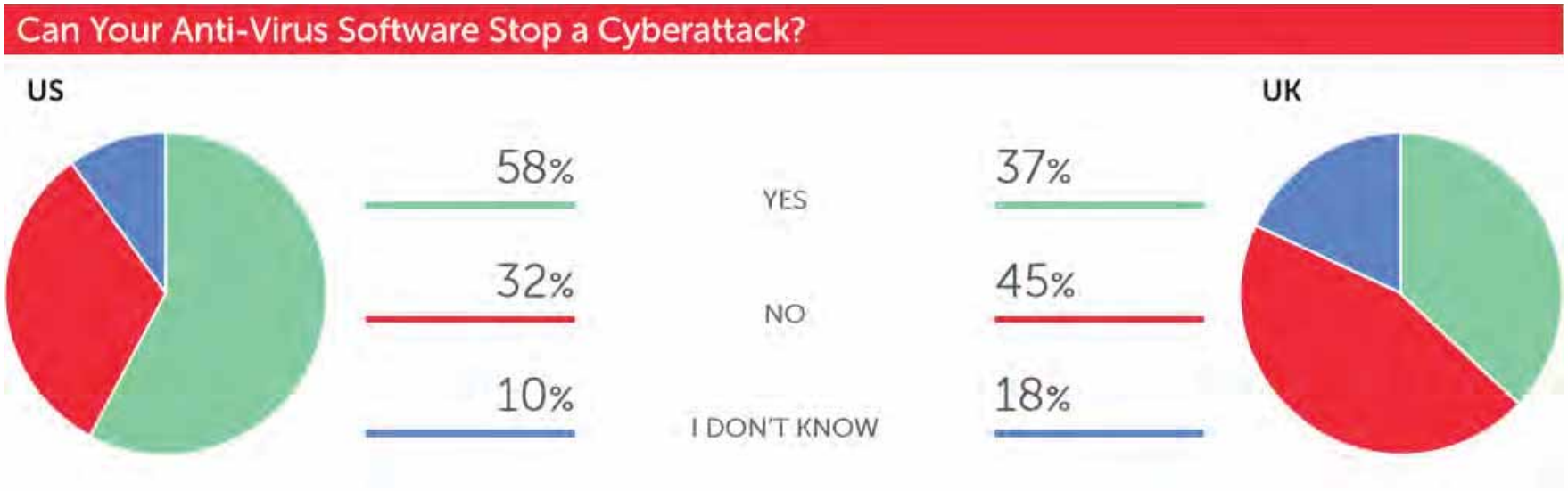
Ransomware

What Is Ransomware?



wombat security technologies

General Knowledge



General Knowledge

Does a Trusted Location = Trusted WiFi?

We presented our survey participants with what we thought was a relatively straightforward question: *If you are in a place you trust — like a nice hotel, local coffee shop, or international airport — can you trust that location's free WiFi service to keep your information secure?* We were surprised by the number of people (particularly those in the US) who have misplaced trust in these networks.

Are Business Pages Approved by Social Platforms Before Being Posted?

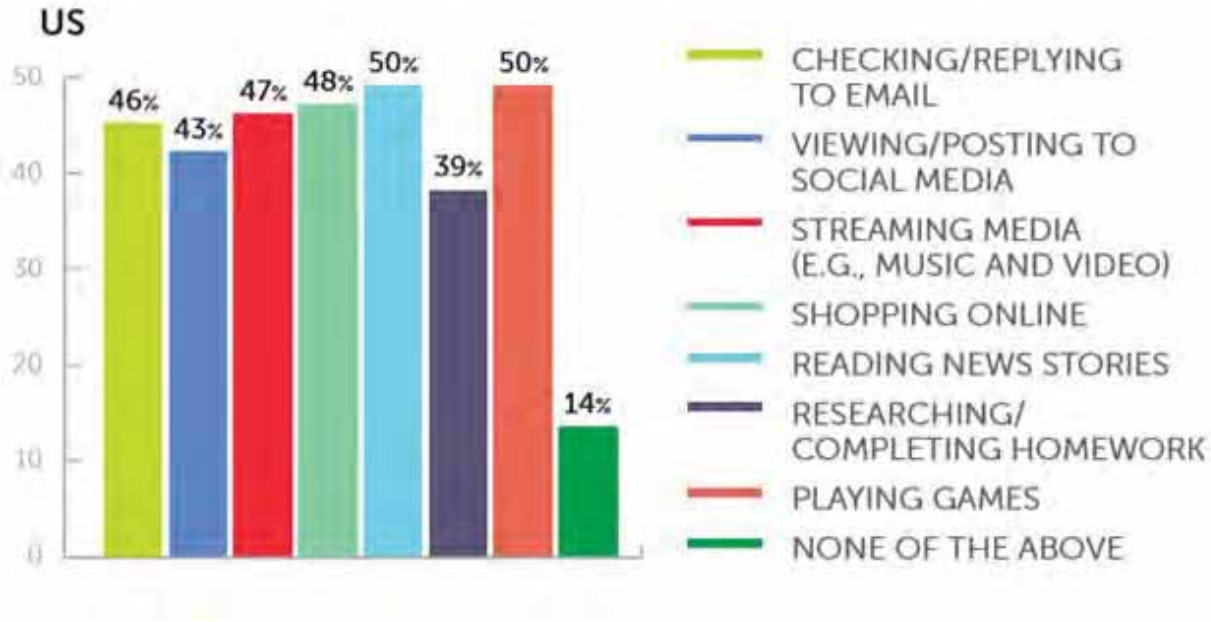
Unfortunately, too many employees believe that platforms like Facebook, Instagram, and Twitter approve business pages before allowing them to be posted (though US employees once again lag behind their UK counterparts).

wombat security technologies

Personal Use of Corporate Devices

What Personal Activities Do You Allow Family Members or Trusted Friends to Perform on Your Corporate Device? *(Multiple responses permitted)*

Well, we admit it: we were floored to see how many employees (particularly those in the US) give their friends and family members access to their corporate devices.



wombat security technologies

State of the Phish 2017

Phishing Threats

What are Companies Experiencing?

76%
reported being the victim of a phishing attack in 2016

Down **10%** from 2015

51%
said the rate of phishing attacks is increasing

Down **15%** from 2015

45%
said the rate of phishing attacks is decreasing

4%
said the rate has stayed the same

44%
experienced phishing through phone calls (vishing) and SMS messaging (smishing)

Decrease of **20%** from 2015

4%
experienced phishing through USB attacks

Decrease of **33%** from 2015

#StateofthePhish

wombat security technologies

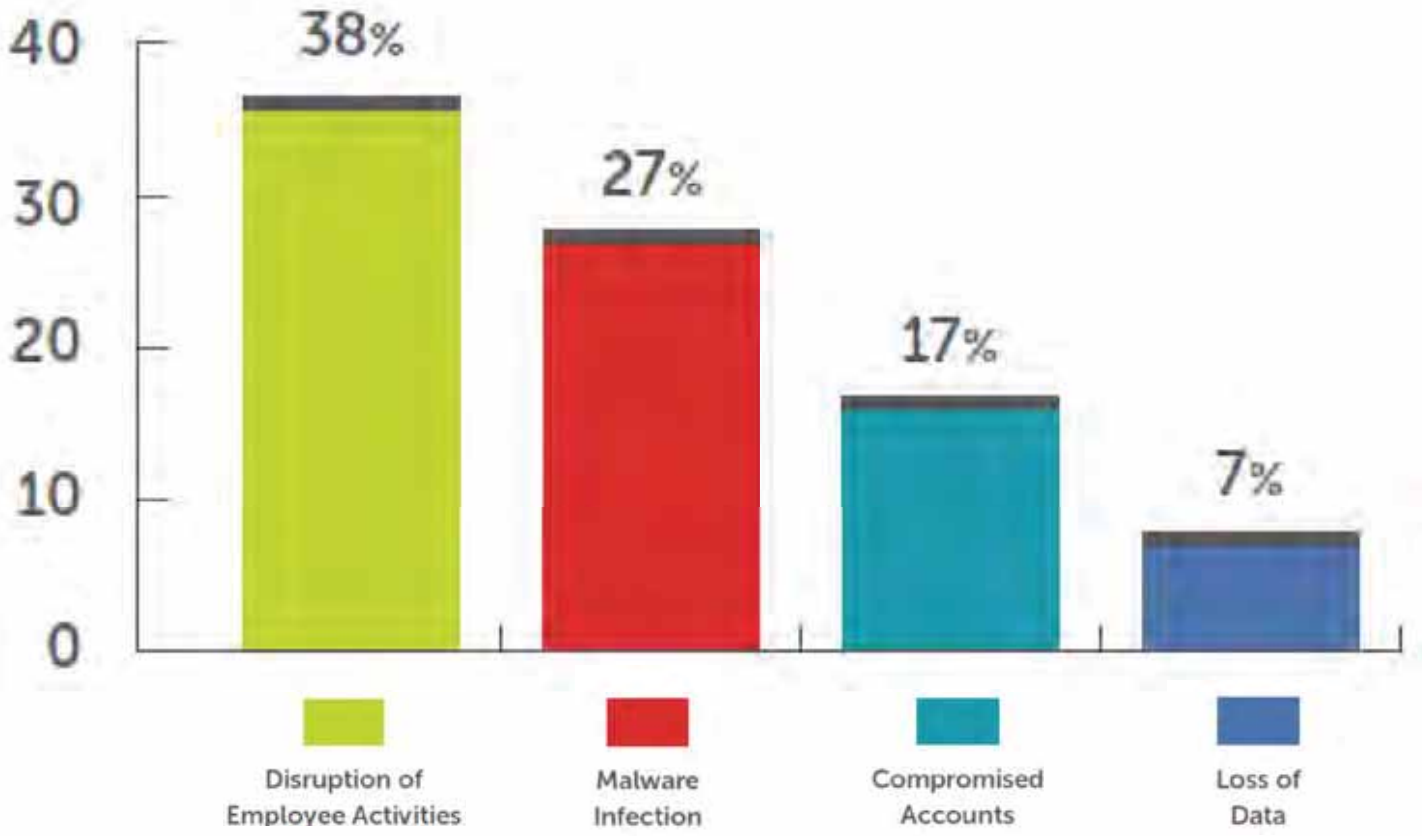
Why Should You Care?

- Phishing attacks are increasing in complexity
- Attackers are targeting the end user
- Increasing reliance on end users to make responsible security decisions
- An increasingly connected and at-risk workforce
- Attacks cost your organization money and time

#StateofthePhish

The Impact of Phishing

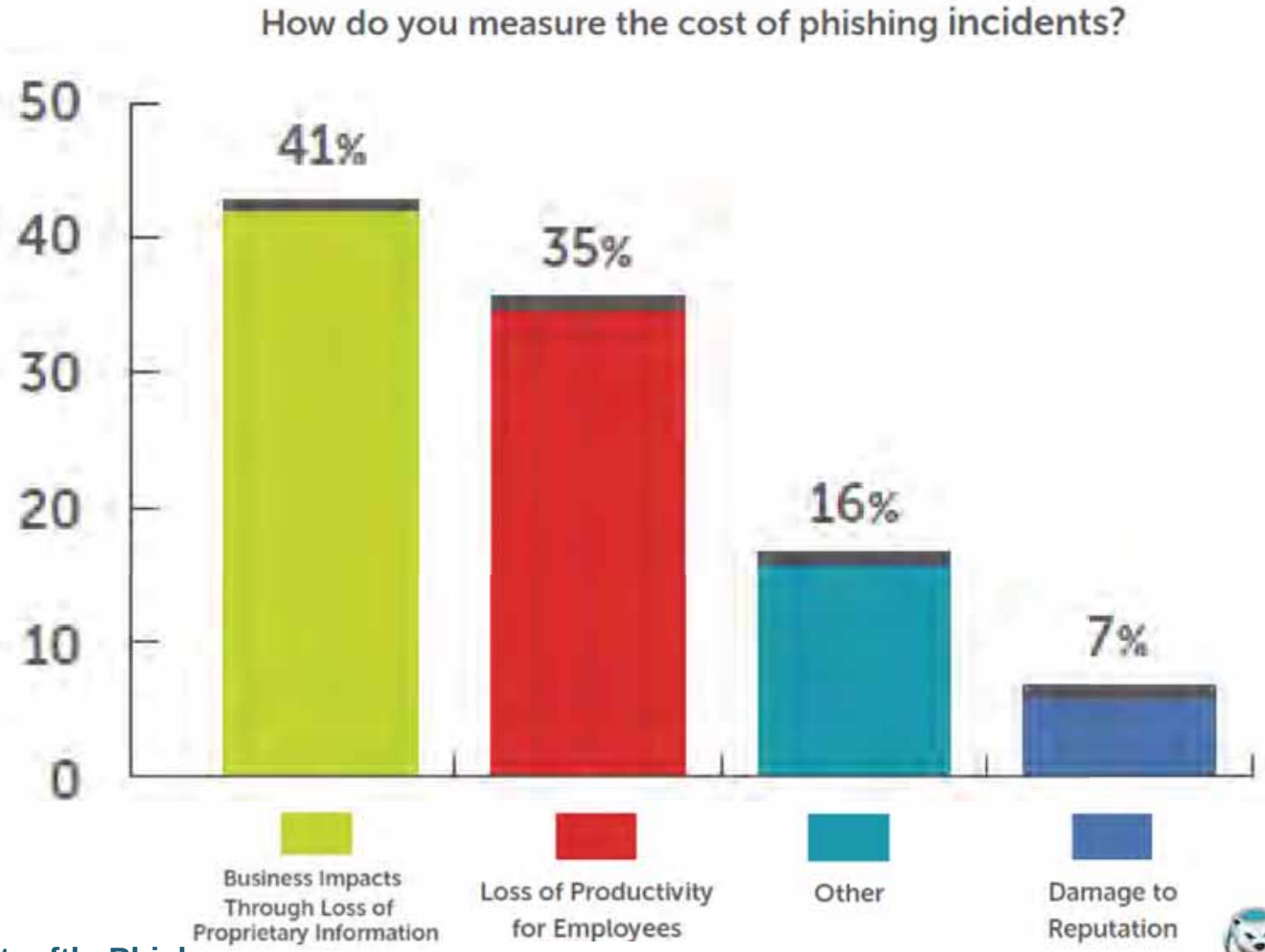
What has the impact of phishing been on your organization? (choose all that apply)



#StateofthePhish

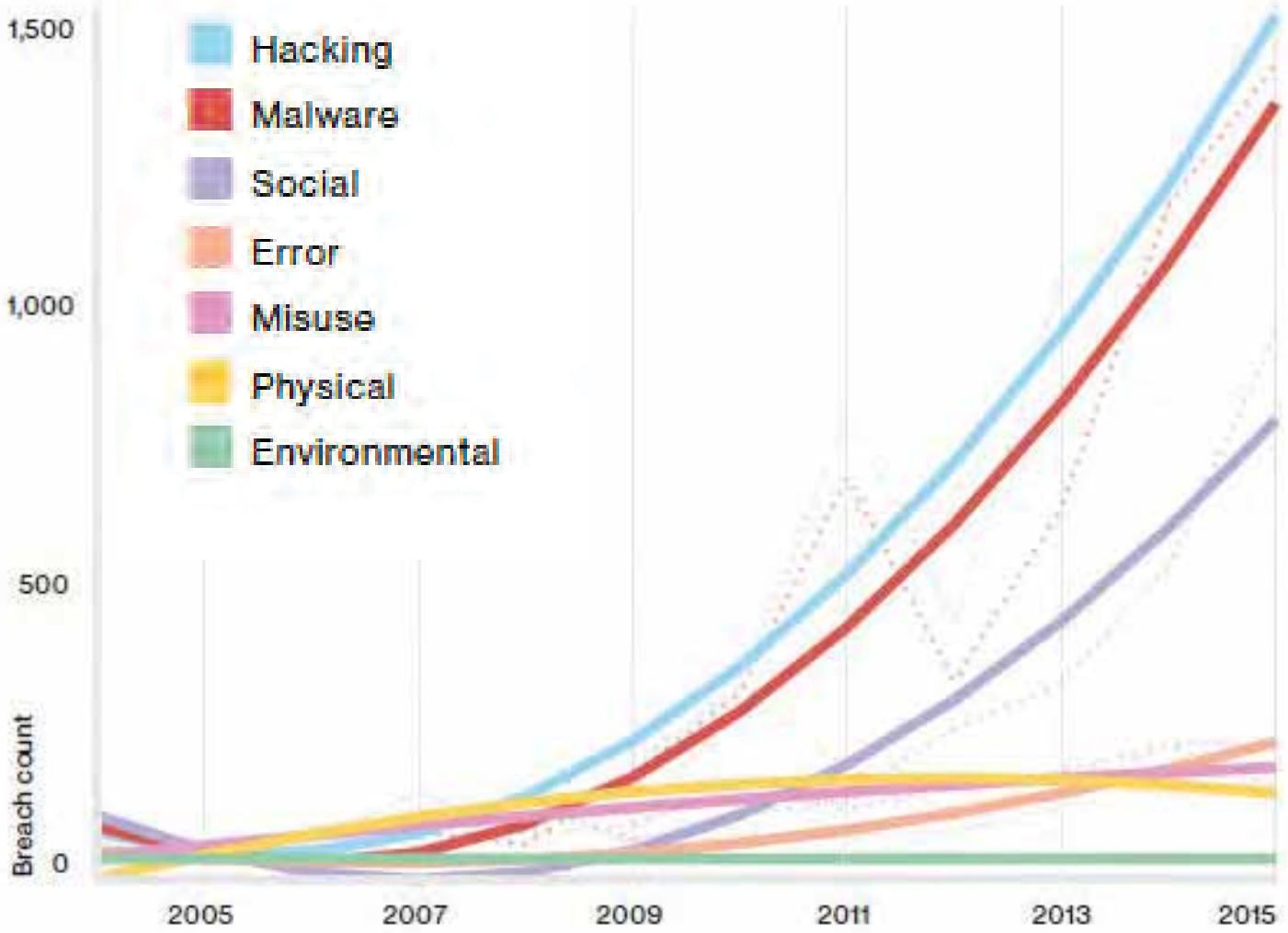
wombat security technologies

The Cost of Phishing



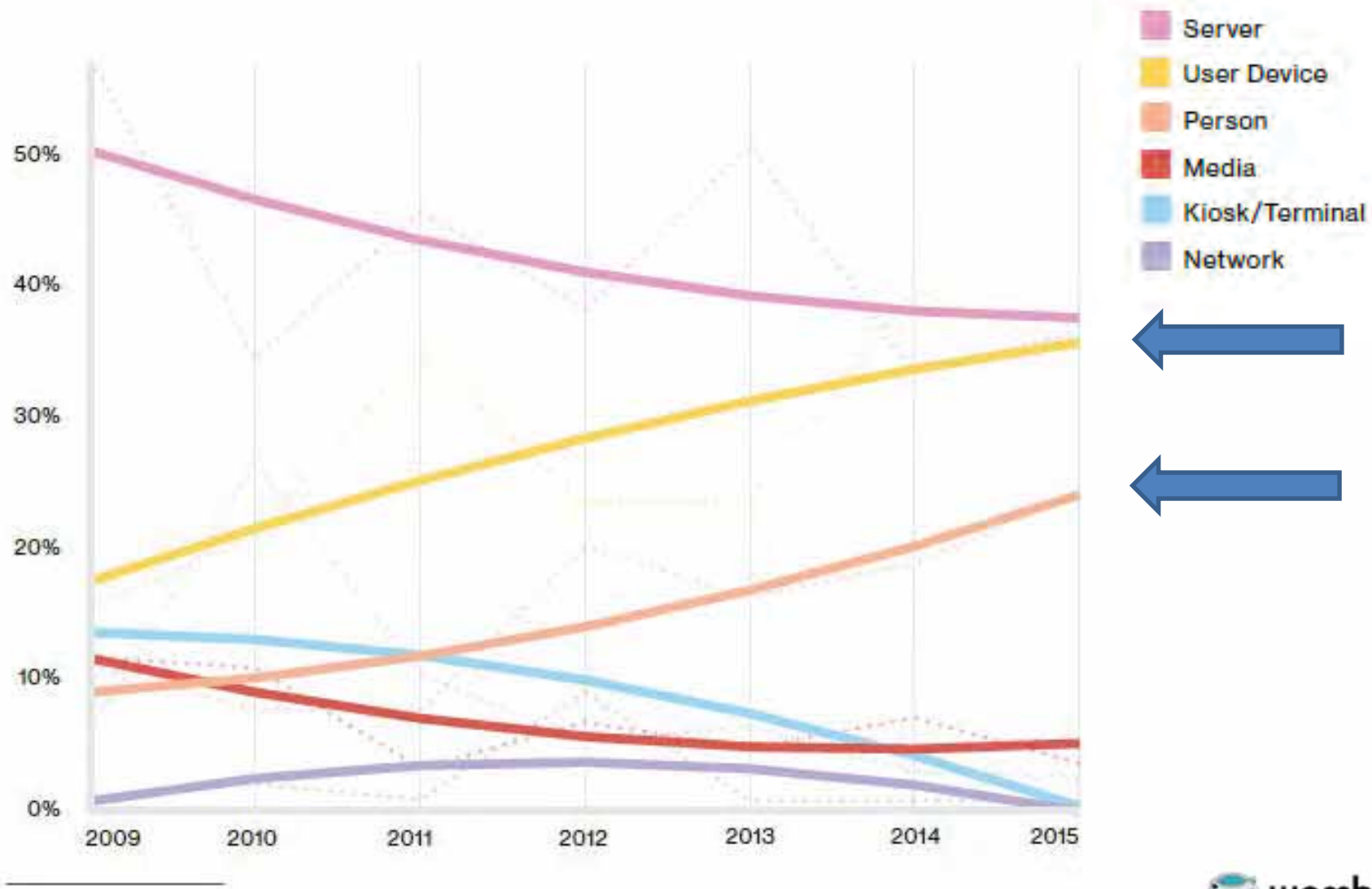
#StateofthePhish

Breaches per Threat Action



2016 Verizon Data Breach Investigations Report

Breaches Per Asset Category



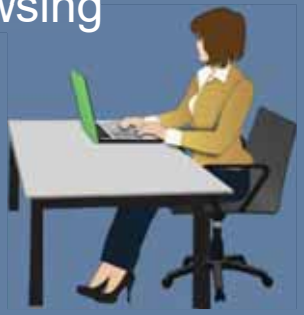
2016 Verizon Data Breach Investigations Report

Phishing Root Cause

Imposter Phone Calls

Roughly 156 million phishing emails are sent globally every day[1]

Unsafe Browsing



Oversharing on Social Networks

[1]Symantec Security Technology and Response Group

wombat security technologies

Beyond the Phish

Beyond the Phish Data

Data compiled from Wombat Security and direct feedback from InfoSec professionals

Wombat Assessment Data

- Analysis of data from nearly 20 million questions asked and answered inside the Wombat Security Education Platform
- Assessment data spans 2014 to 2016

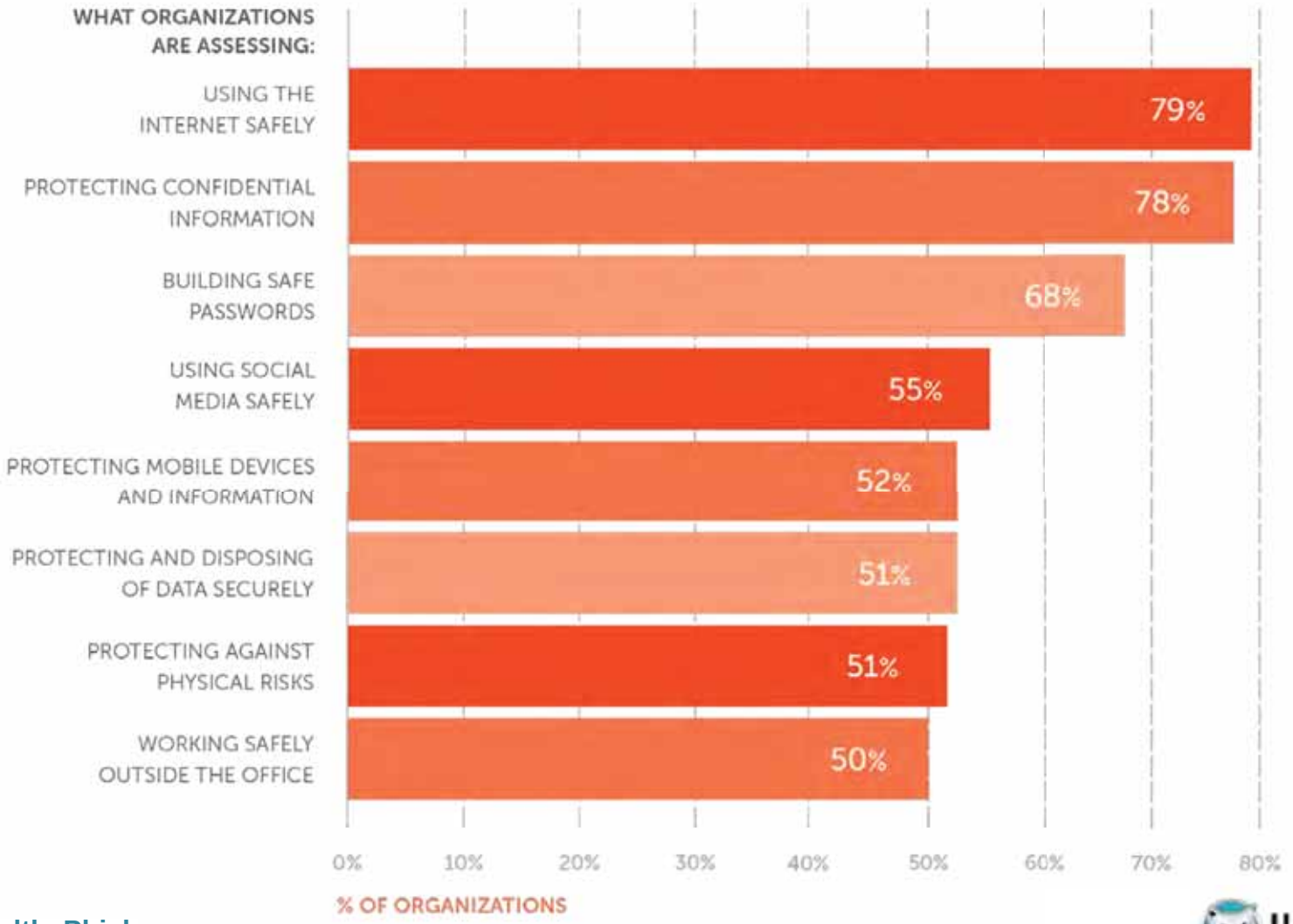
InfoSec Professionals Survey

- Feedback from over 300 surveys
- Over 15 different industries

#BeyondthePhish

wombat security technologies

Topics Security Teams Assess On

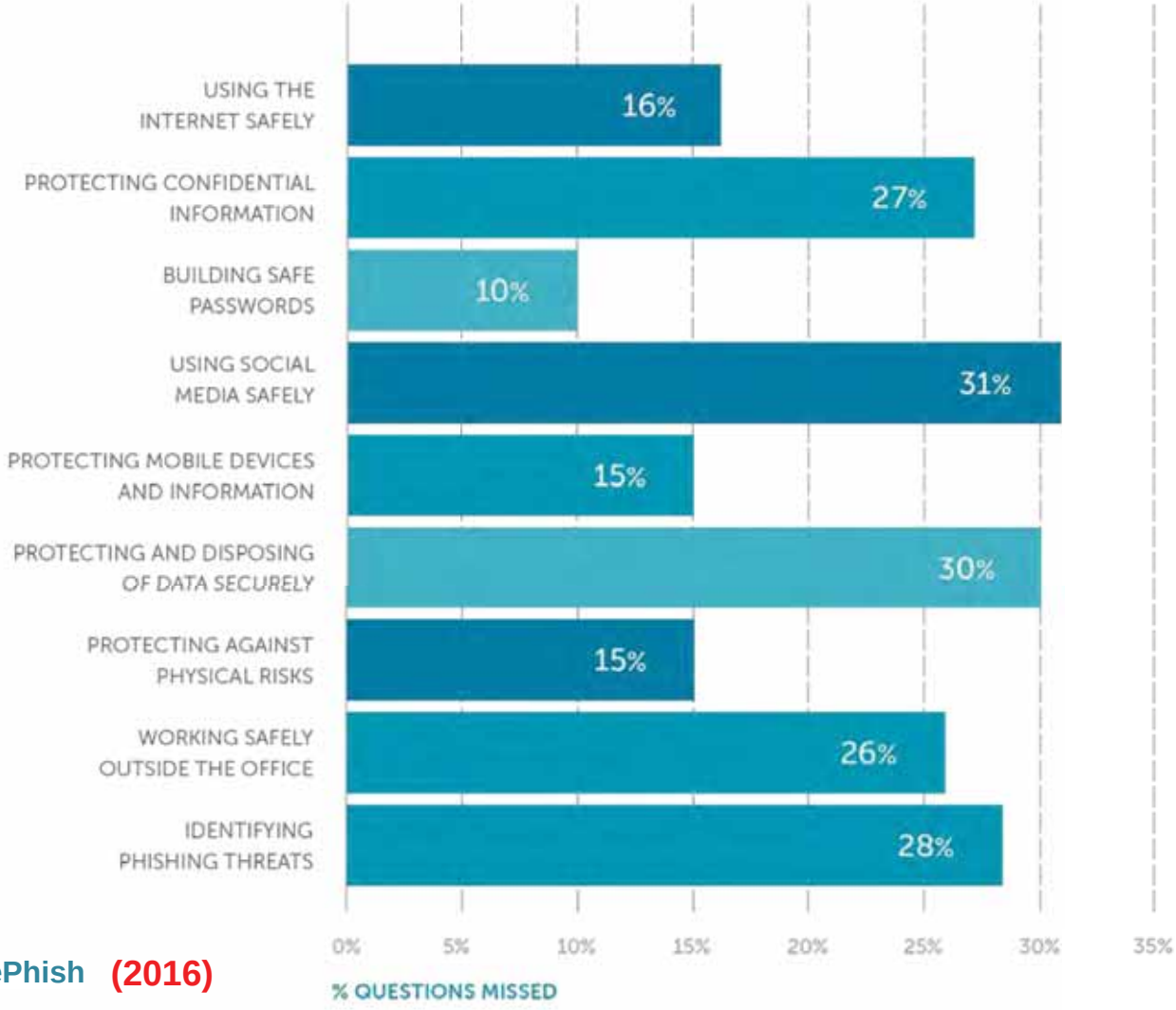


#BeyondthePhish

wombat security technologies

Where are Users Strong or Weak?

% incorrect answers



#BeyondthePhish (2016)

wombat security technologies

Using Social Media Safely

- Most missed questions were around being vigilant in recognizing if you are dealing with a friend's fake profile and posts
  - Look for posts that are out of the ordinary, spelling and grammar errors

- 70% of social media scams were shared manually (compared to only 2% in 2013)*

* SYMANTEC CORPORATION Study: Internet Security Threat Report 2015

wombat security technologies

Using Social Media Safely

55% **Assess on using Social Media safely**

76% **Allow access to Social Media on work devices**

#BeyondthePhish

wombat security technologies

Using Social Media Safely

31%
QUESTIONS MISSED

55% **Assess on using Social Media safely**

76% **Allow access to Social Media on work devices**

#BeyondthePhish

wombat security technologies

Protect and Dispose of Data Securely

What Types of Questions were Asked?

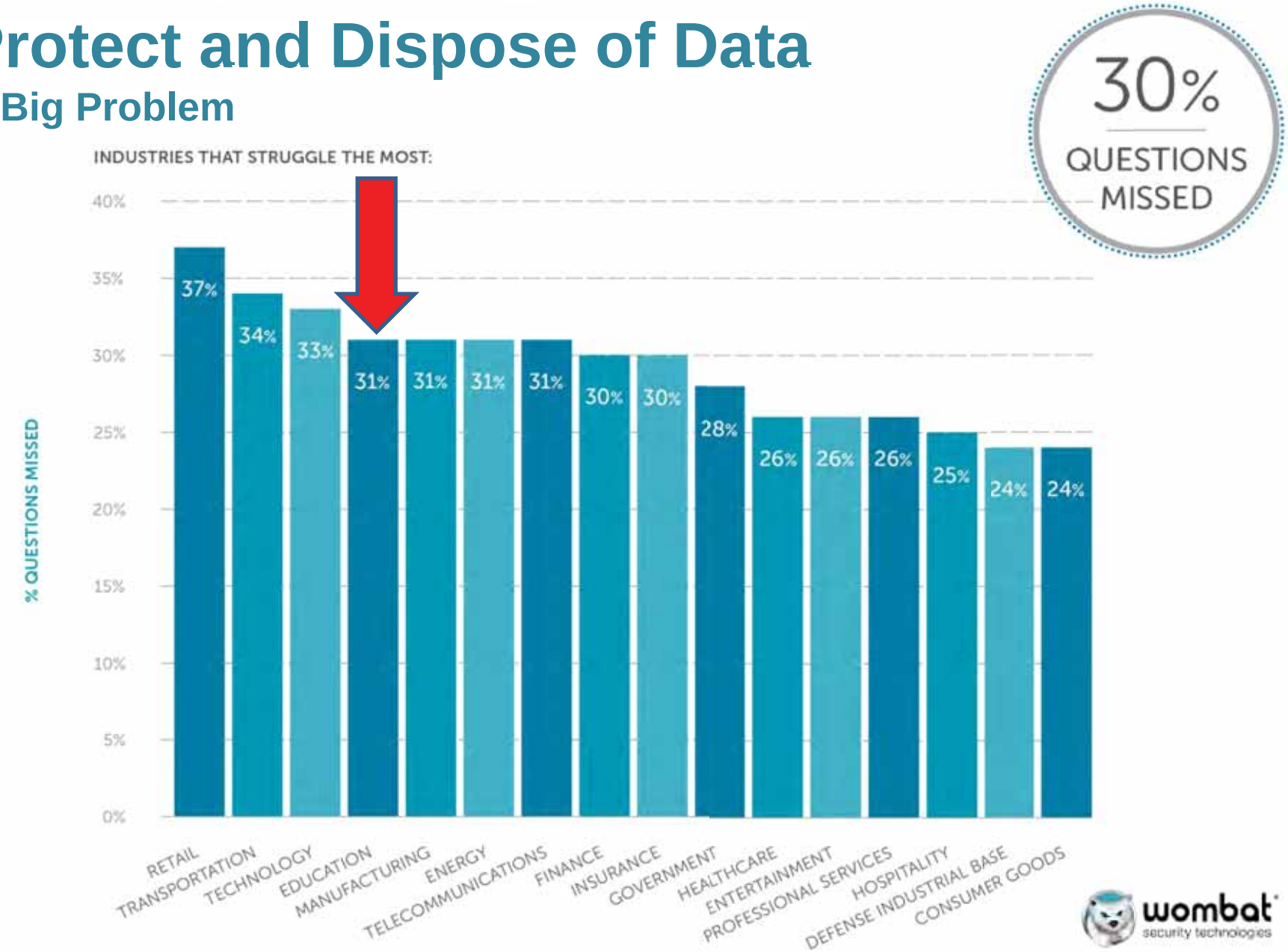
- Lifecycle of data - from creation to deletion
- Handling PII
- Using USBs
- Deleting files from hard drives
- Securing work devices

One of the common misconceptions from end users is that there is technology in place that will protect them from being hacked so they did not need to be as vigilant

wombat security technologies

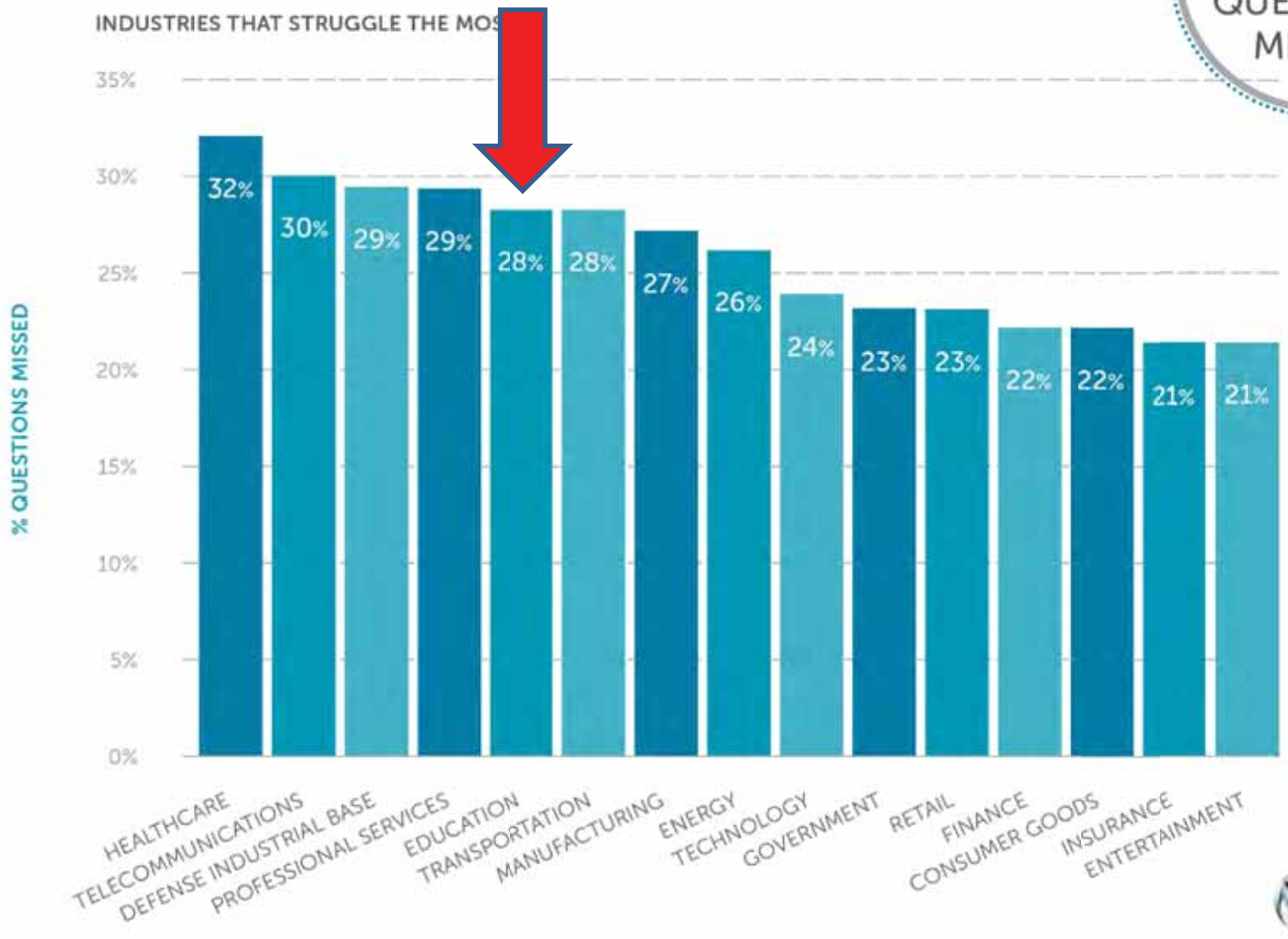
Protect and Dispose of Data

A Big Problem



Protect Confidential Information

Another Big Problem



wombat security technologies

Work Safely Outside the Office

- Only 50% are assessing around this topic
- Most missed questions were around safely connecting to WiFi

wombat security technologies

Work Safely Outside the Office

- Only 50% are assessing around this topic
- Most missed questions were around safely connecting to WiFi

How confident are you that employees don't connect to public WiFi networks without a protected connection such as a VPN?

52% NOT VERY CONFIDENT

32% NEUTRAL

17% CONFIDENT

wombat security technologies

Work Safely Outside the Office

- Only 50% are assessing around this topic
- Most missed questions were around safely connecting to WiFi

How confident are you that employees don't connect to public WiFi networks without a protected connection such as a VPN?

52% NOT VERY CONFIDENT

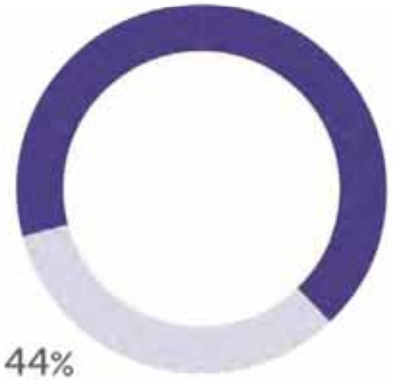
32% NEUTRAL

17% CONFIDENT

Do you have a security policy/guideline for employees to follow while traveling?

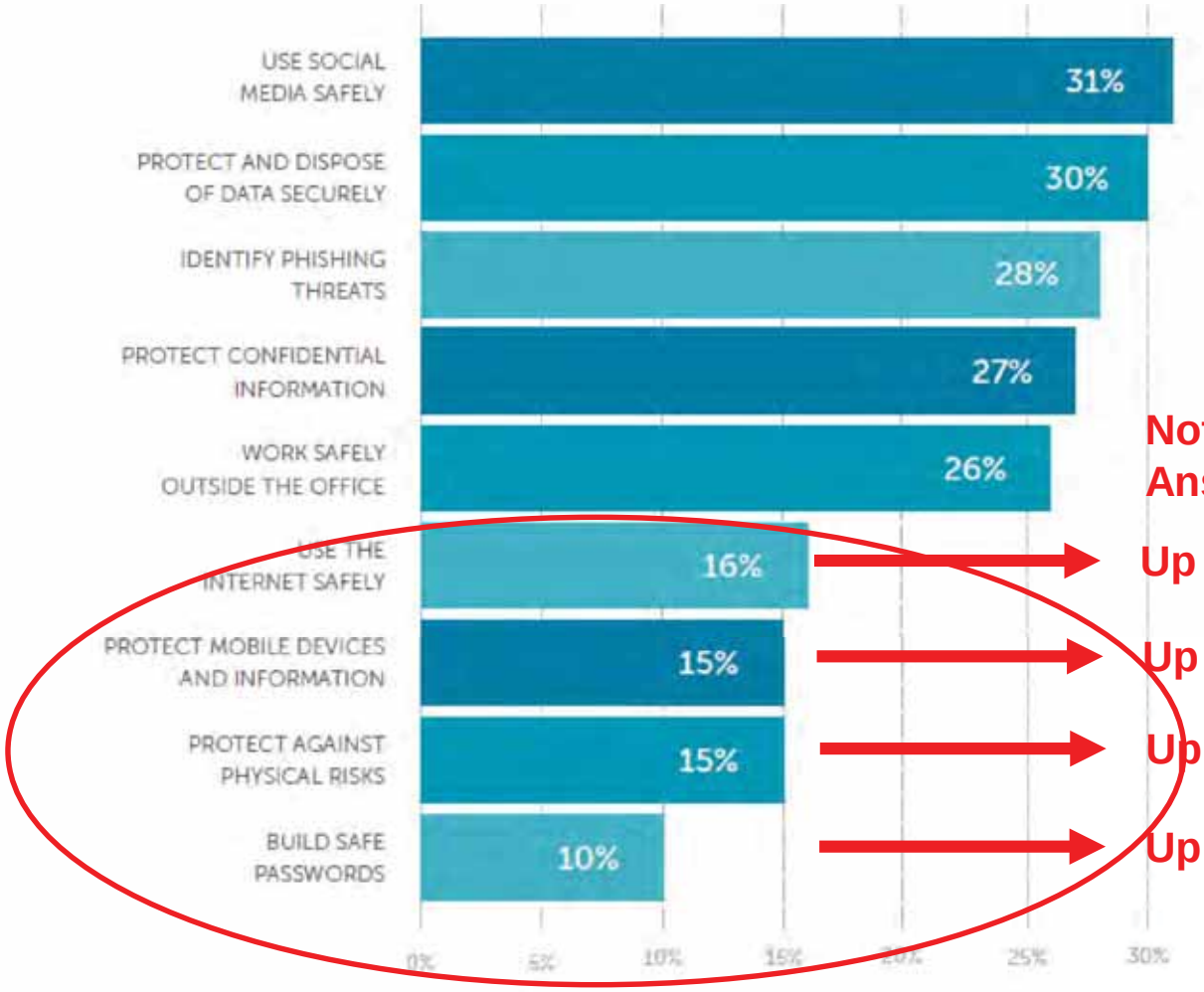
56% YES

44% NO



wombat security technologies

Where do End Users Succeed?



Note: Reflects Incorrect Answers

Up to 19% for 2017

Up to 24% for 2017

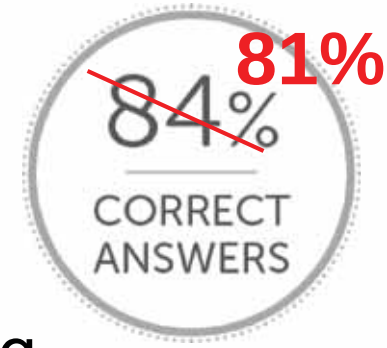
Up to 18% for 2017

Up to 12% for 2017

#BeyondthePhish

wombat security technologies

Use the Internet Safely



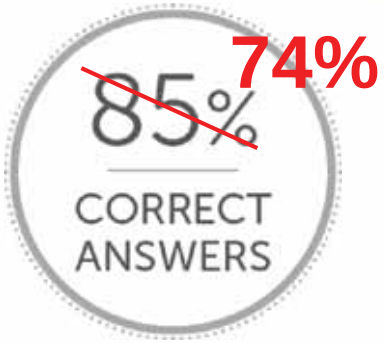
- 79% are assessing around this topic
- Defense Industrial Base did the best, getting 90% correct around this topic

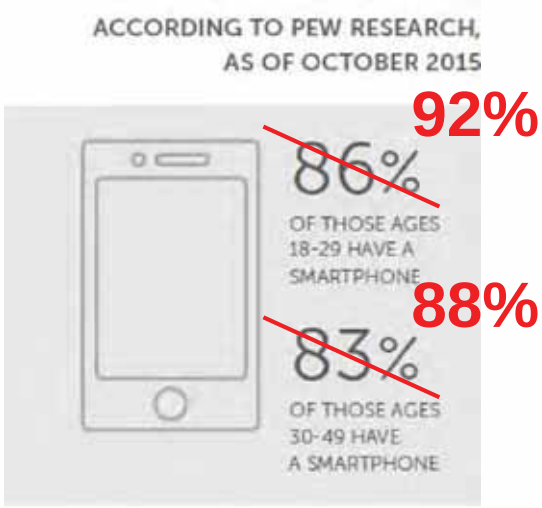
What is your confidence level that employees understand safe practices for browsing the internet (such as logging out of web apps before closing, etc)?

31%	52%	17%
NOT VERY CONFIDENT	NEUTRAL	CONFIDENT

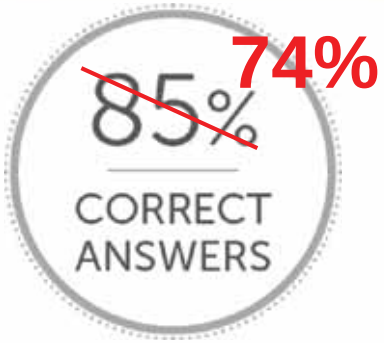
wombat security technologies

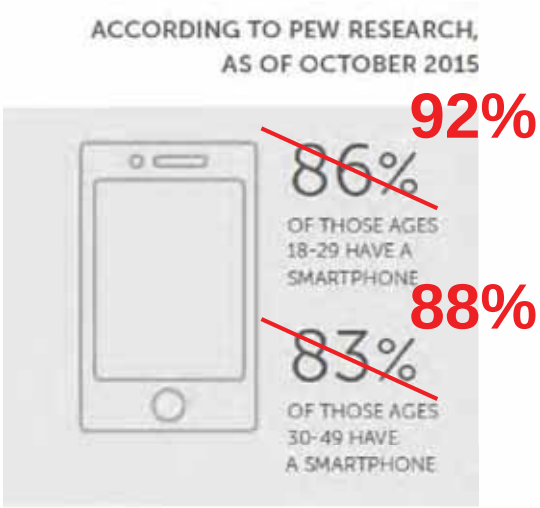
Protect Mobile Devices and Information

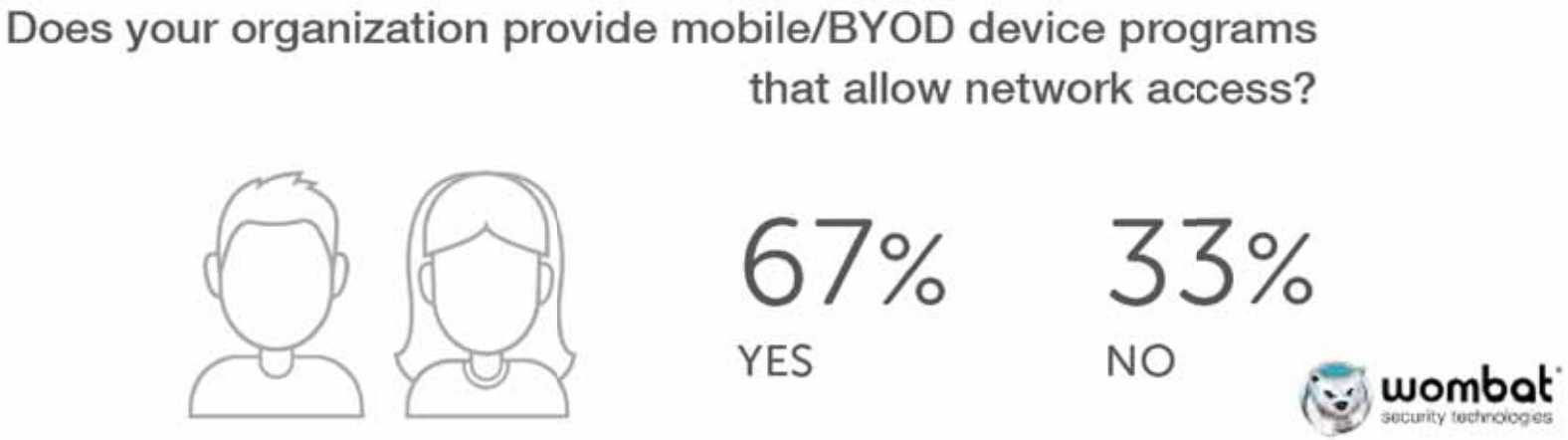




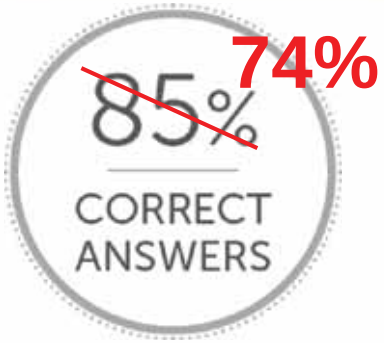
Protect Mobile Devices and Information

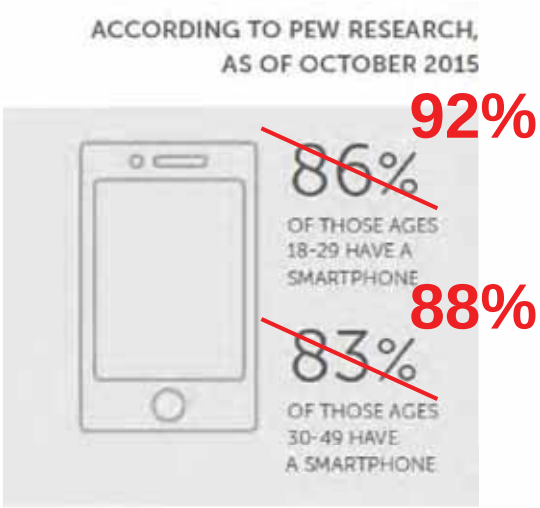




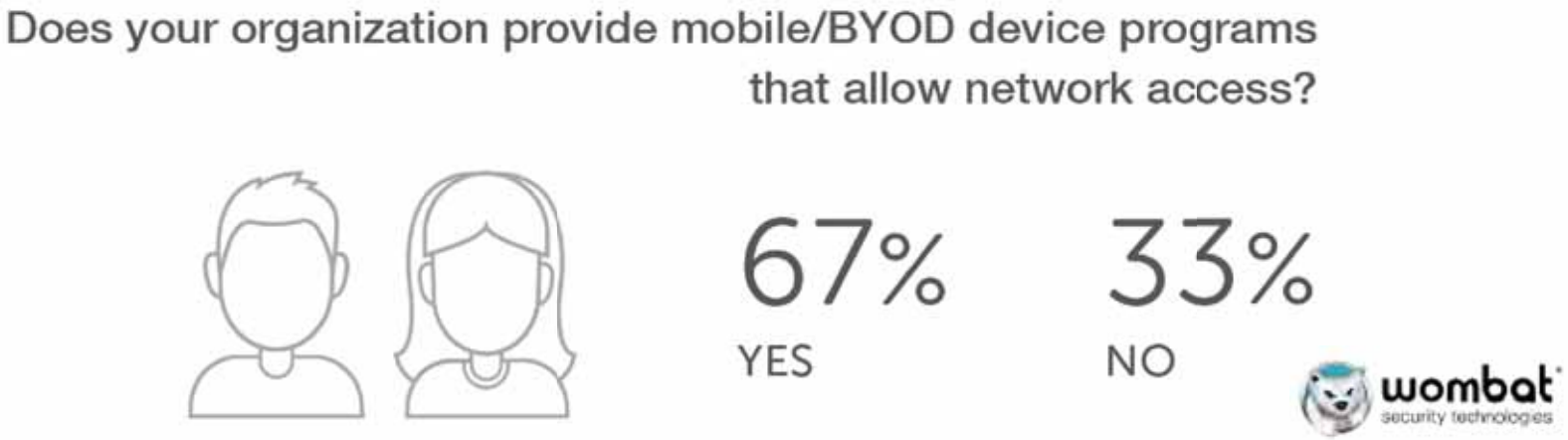


Protect Mobile Devices and Information

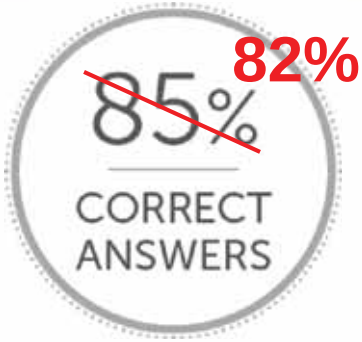




- Only 52% are assessing around this topic
- Most missed questions were around connecting to Bluetooth



Protect Against Physical Risk



- 51% are assessing around this topic
- Top questions missed around computer safety in the office
  - locking your computer when you walk away
  - locking devices in your drawer overnight
- 55% of theft-related incidents occurred within the victim's work area*

*2015 Verizon Data Breach Investigations Report

wombat security technologies

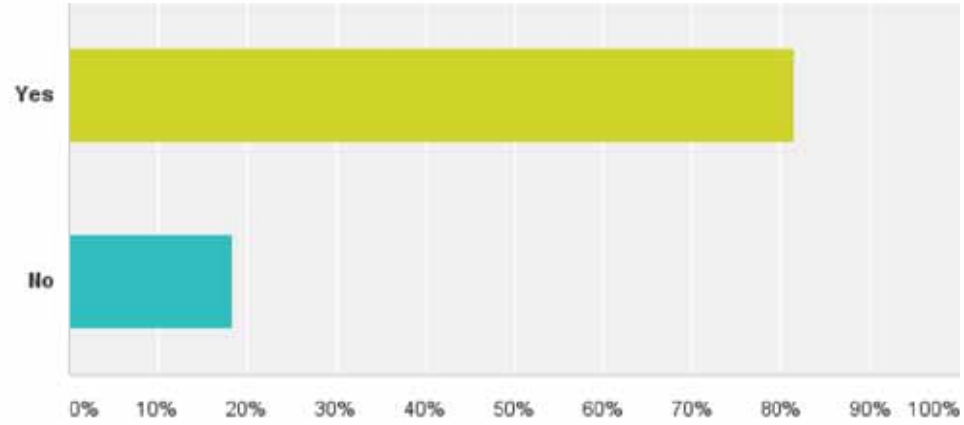
Build Better Passwords

- 68% assess on this topic
- Top questions missed around not using personal information to create passwords like birth dates or wedding dates
- Entertainment industry did the best in this topic, getting 93% of all questions correct.

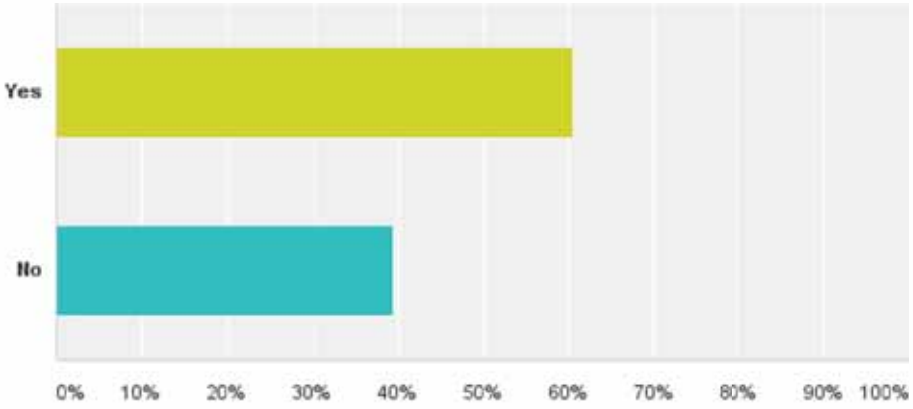
wombat security technologies

Build Better Passwords

Do you enforce strong password policies?



Do you use two-factor authorization?

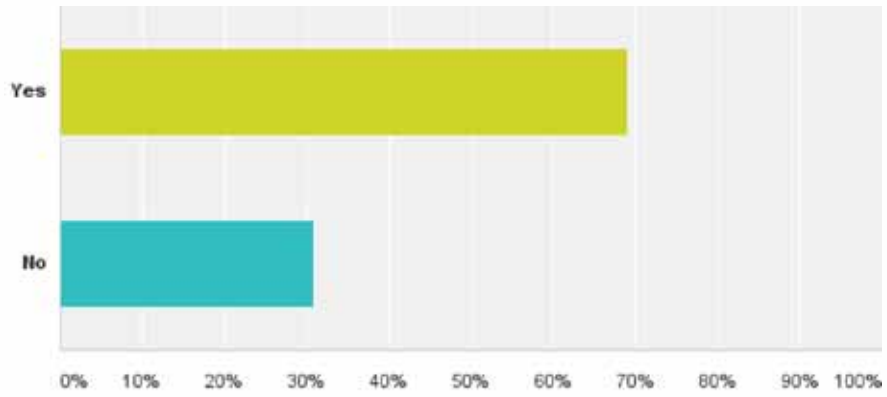


wombat security technologies

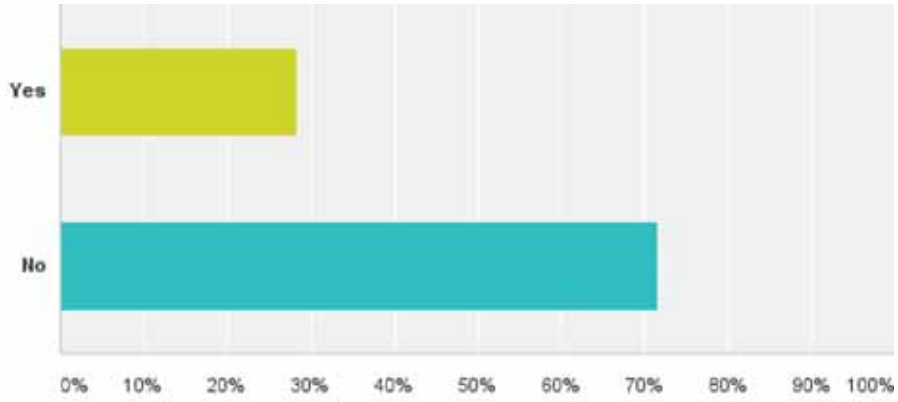
Measurement is Key

- Assessing allows you to:
  - Identify problem areas
  - Have something to measure progress against

Wombat Customers



Non-Customers



#BeyondthePhish

wombat security technologies

Simulated Attack vs. Assessments in 2017

Healthcare

18%

CLICK RATE IN
SIMULATED PHISHING ATTACKS

VS.

26%

QUESTIONS MISSED IN ASSESSMENTS

Government

14%

CLICK RATE IN
SIMULATED PHISHING ATTACKS

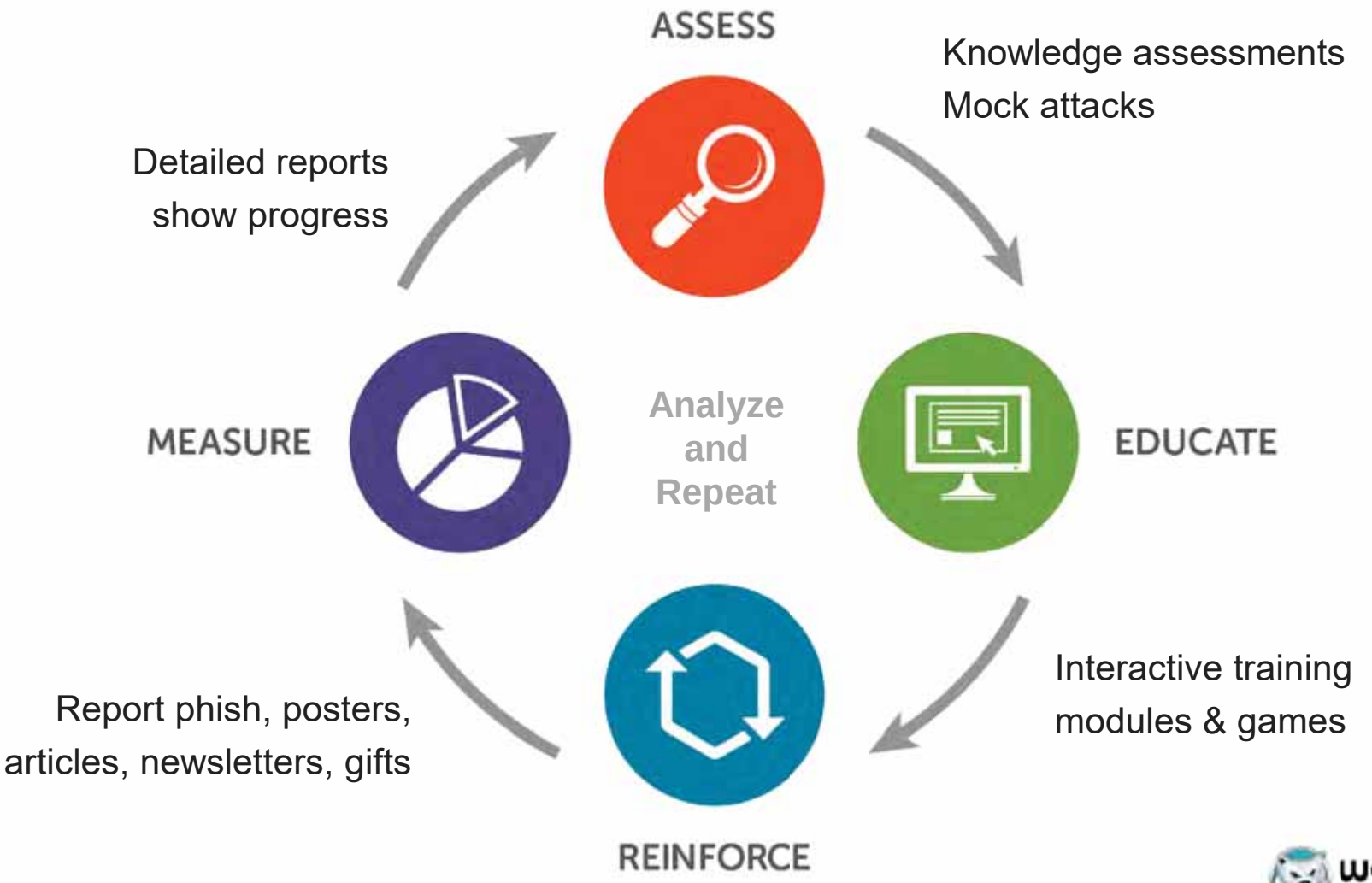
VS.

24%

QUESTIONS MISSED IN ASSESSMENTS

wombat security technologies

Continuous Training Methodology



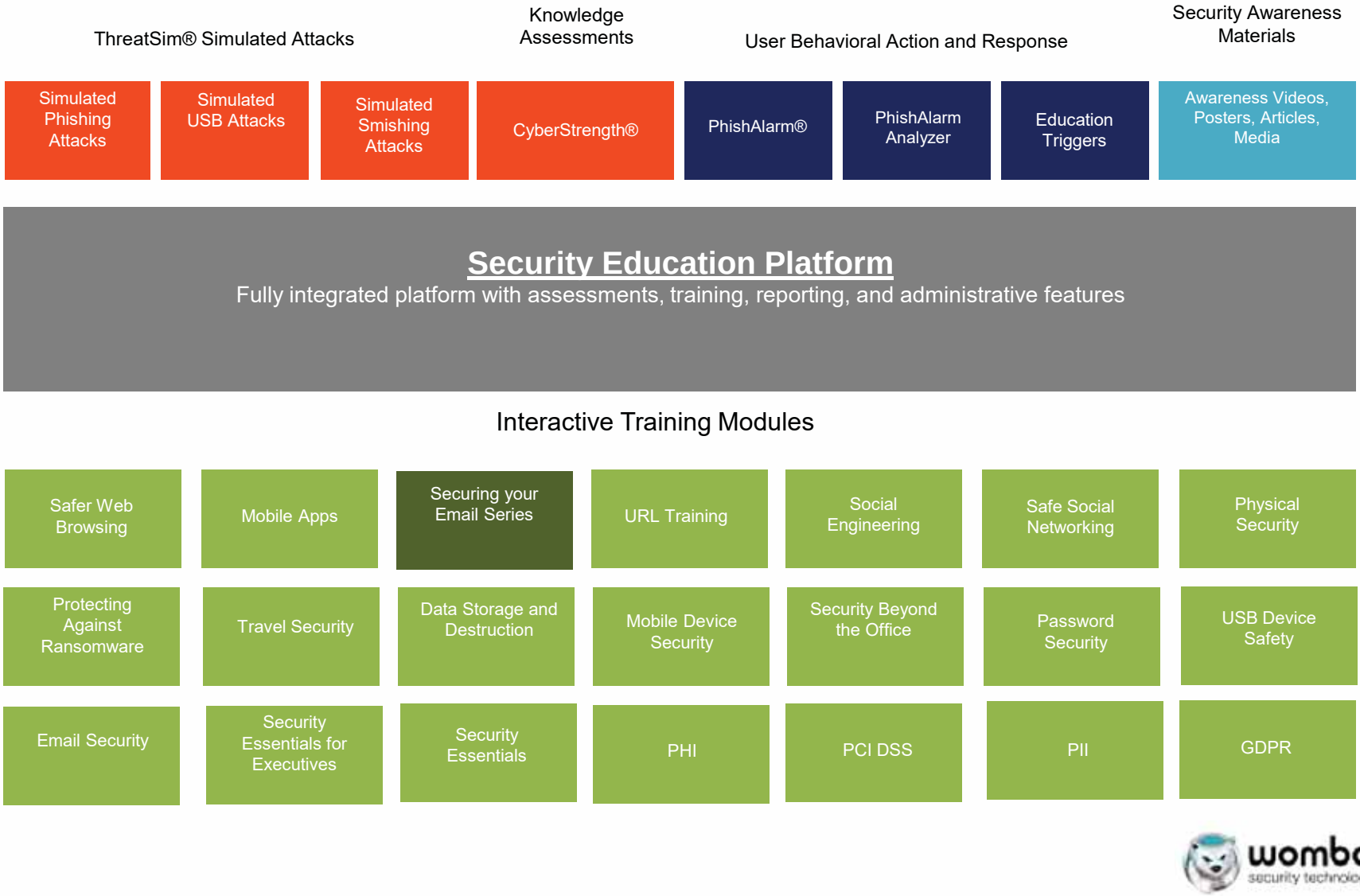
wombat security technologies

Application of Learning Science Principles

- Present concepts and procedures together
- Bite-sized lessons
- Learn by doing
- Story-based environment
- Provide immediate feedback
- Create teachable moments
- Use conversational tone
- Collect valuable data

wombat security technologies

Wombat Portfolio



Key Takeaways

- Phishing attacks are becoming more complex/targeted and incorporating other threat vectors
- Emerging/changing attacks (and varying user performance) requires a continuously evolving program. Set-it-and-forget-it won't suffice.
- Question-based assessments will expose user vulnerabilities 1.5 – 2x more than attack-based assessments… *AND* provide visibility into users' specific vulnerabilities
- Informing users ≠ equipping users to ***behave*** differently

wombat security technologies

Questions?