Emerging Trends in Technology Fraud Prevention & Detection

Navigating Top 10 Technology Risks

1. Cybersecurity
2. Information Security
3. IT Systems Development Projects
4. IT Governance
5. Outsourced IT Services
6. Social Media Use
7. Mobile Computing
8. IT Skills Among Internal Auditors
9. Emerging Technologies
10. Board and Audit Committee Technology Awareness

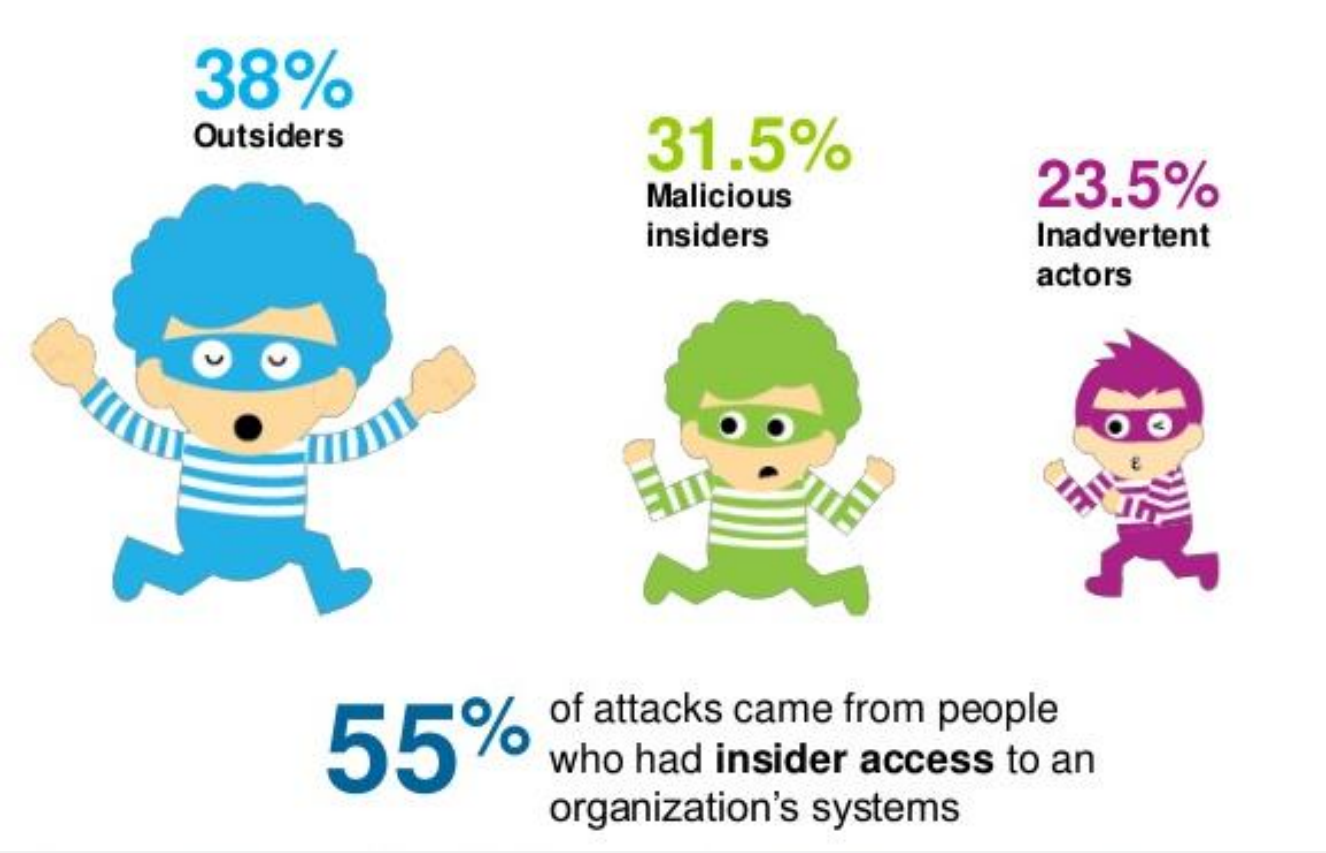
The IIA Research Foundation | CBOK
The Global Internal Audit Common Body of Knowledge

14,518 responses
166 countries
23 languages

www.theiia.org/goto/CBOK


The Challenges Ahead

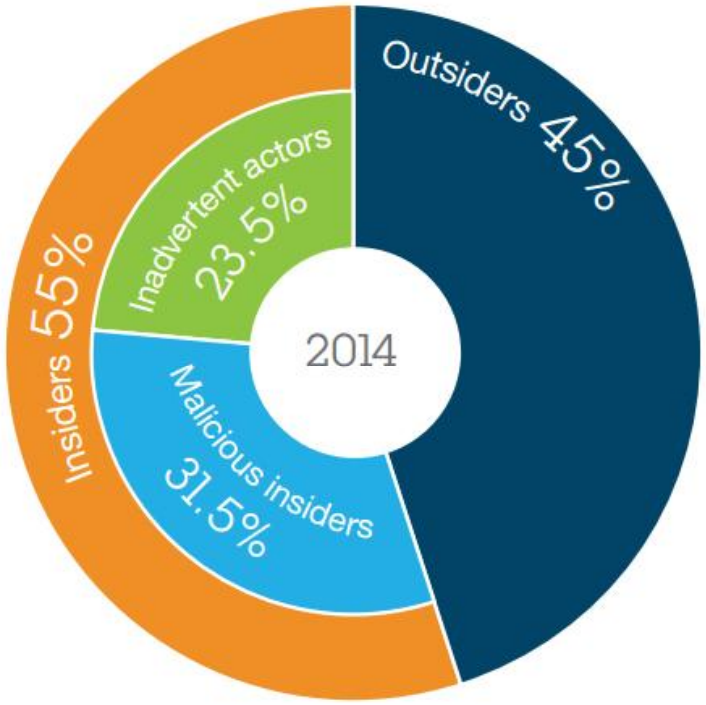
External vs Internal Threats (1)

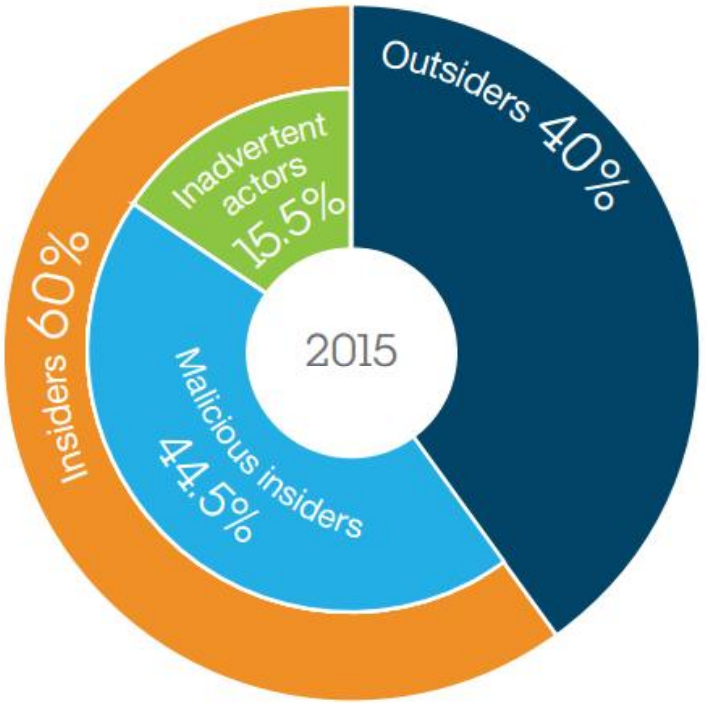


While only 38% attacks came from outsiders

Source:IBM ® X-Force ® Research

External vs Internal Threats (2)





In 2015, **60 percent** of all attacks were carried out by **insiders**, either ones with malicious intent or those who served as **inadvertent actors**. In other words, they were instigated by people you'd be likely to trust. And they can result in **substantial financial and reputational losses**.

Source:IBM ® X-Force ® Research

Dark Web: How does it look like?

Data Populations

90%

7.9 Zetta bytes

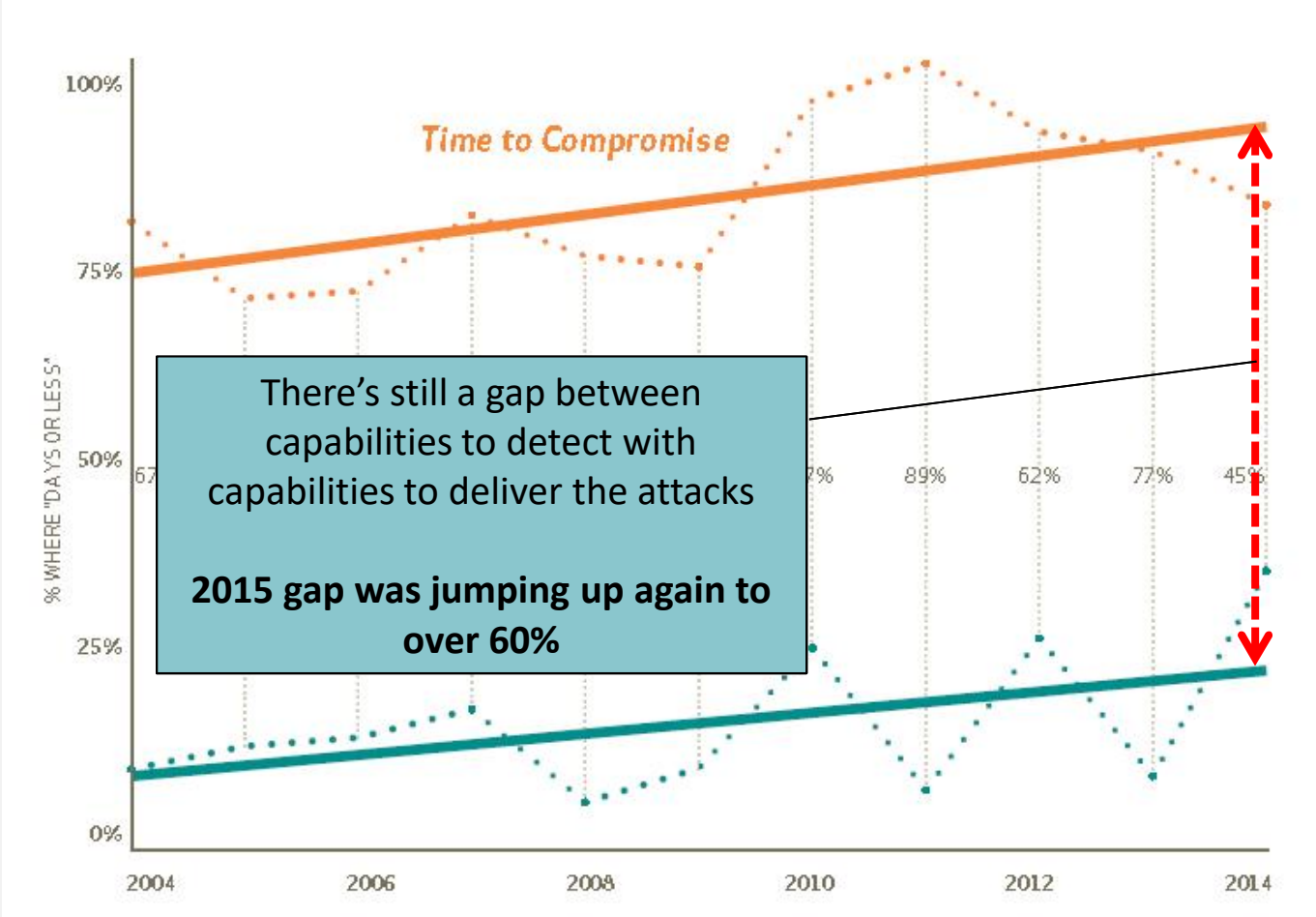
Visible to Browser

3%

Un-indexed, Anonymous TOR/I2P hashed table system to hide database information

Source: Deepwebtech.com

Detection Gap



The defender-detection deficit (range in one-day)

Source: VerizoneData Breach Investigation Report (DBIR)

Know Your Customer

Millennials, also known as Generation Y (after Gen X) and Generation C (for Connected), should perhaps be called Generation Leaky

Recent Dark Reading posting that Milliennials, “have no interest in protecting their data” (Chris Rouland)

They will pay double for organic bread, but they place seemingly no value on the integrity and security of their personal identifiable information

Source:http://www.csoonline.com/article/2884638/security-awareness/millennials-becoming-known-as-generation-leaky.html

#1 Cyber Security: a New Battlefront

Big one

Hackers did indeed cause Ukrainian power outage, US report concludes

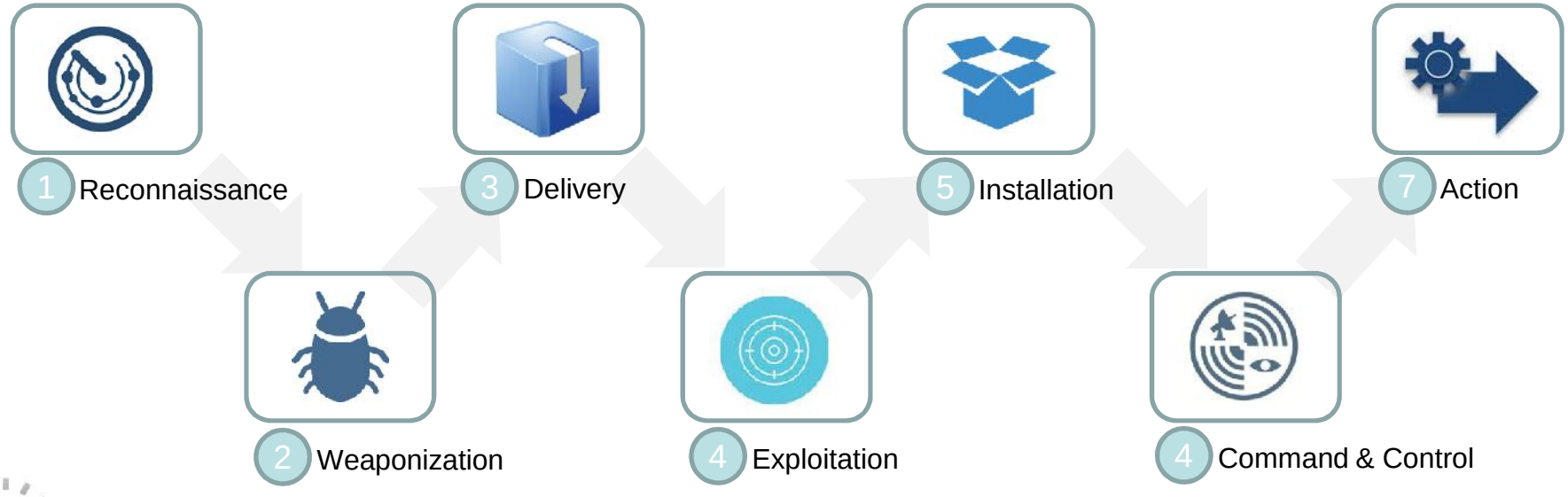
DHS officials say well-coordinated hack cut power to 225,000 people.

by **Dan Goodin** - Feb 26, 2016 8:14pm CET

Share Tweet Email 32

Small (but troublesome) one

Cyber Kill Chain
The Sooner The Better



Source: Darkreading.com

Typical Mobile Apps

1. Client Apps (Android, IOS, BB, WindowsPhone)
2. Browser based Apps (HTML5, CSS, etc)
3. SMS & USSD based Apps
4. NFC Apps (Contactless Smart Card)
5. Value Added Service (VAS) Apps, STK
6. Various Apps
   - MicroATM/POS Apps
   - QR Code
   - Telematic Apps

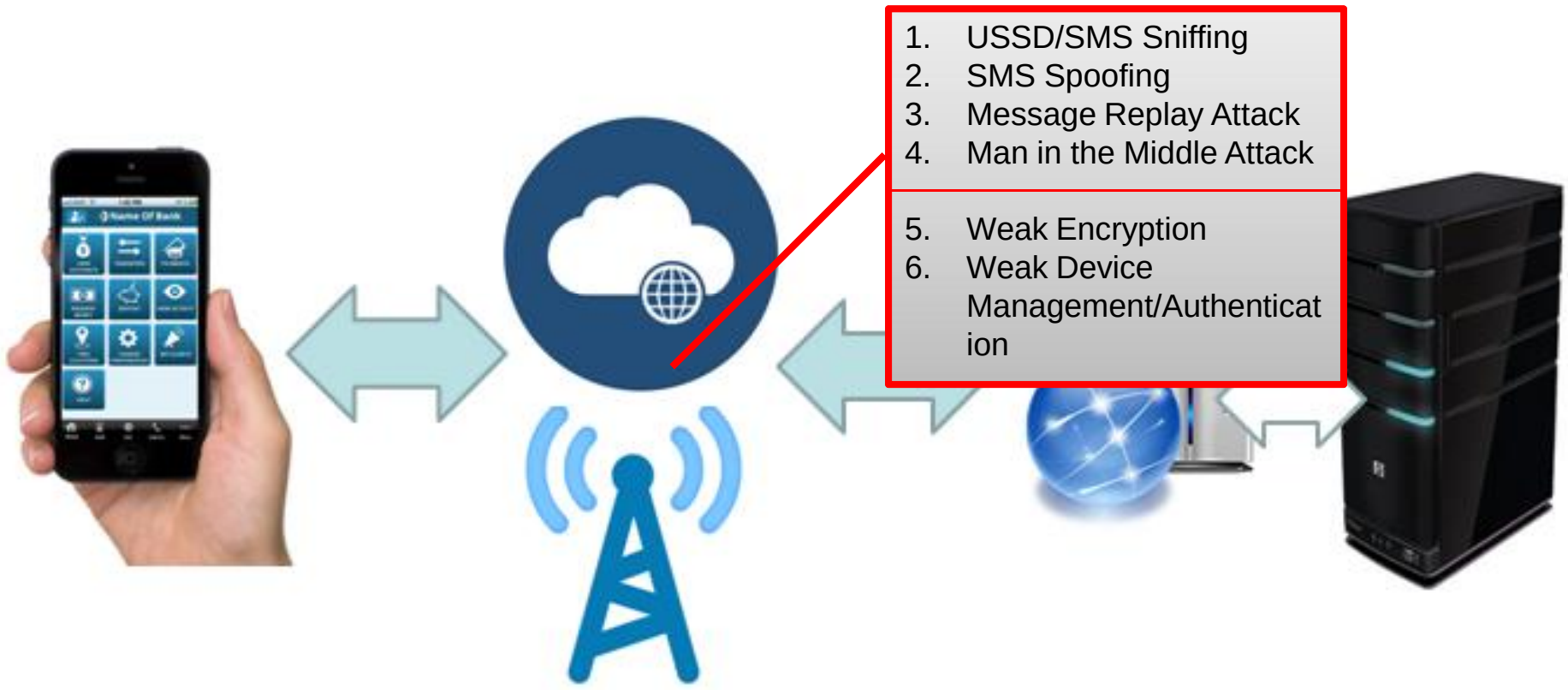
Typical Mobile Application Threats & Vulnerabilities

1. Fake Application
2. Malware Attack – Phone takeover – Insecure Application Permission
3. Smshing, Phishing
4. Man in the Middle (MITMobile, MITBrowser, Zeus in the Mobile)
5. Stolen Devices
6. Spyware, Keylogging

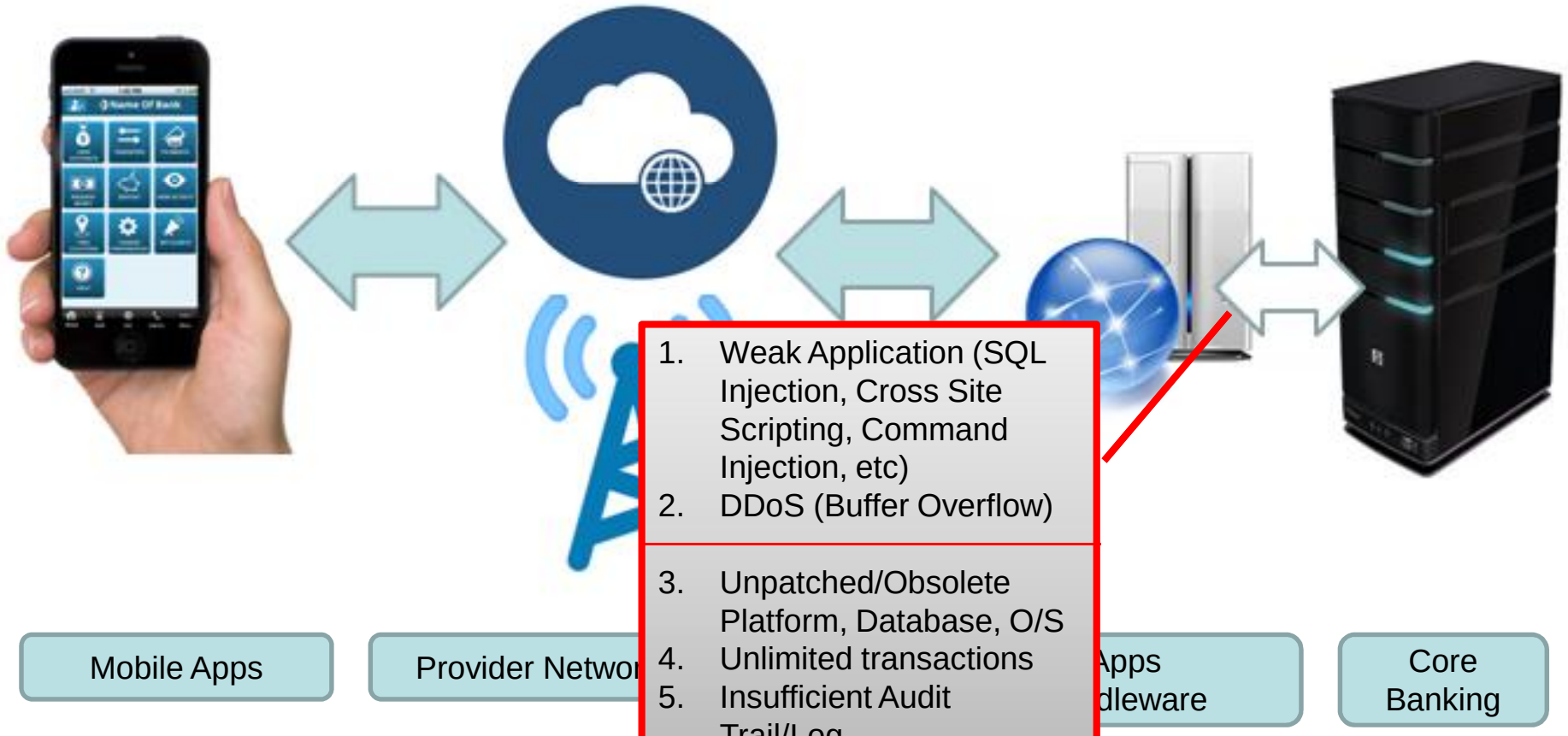
7. Weak User Authentication
8. Weak Device Management/Authentication
9. Rooted/Jailedbreak Device
10. Social Engineering

Mobile Apps | Provider Network/Internet | Mobile Apps Server/Middleware | Core Banking

Typical Mobile Application Threats & Vulnerabilities

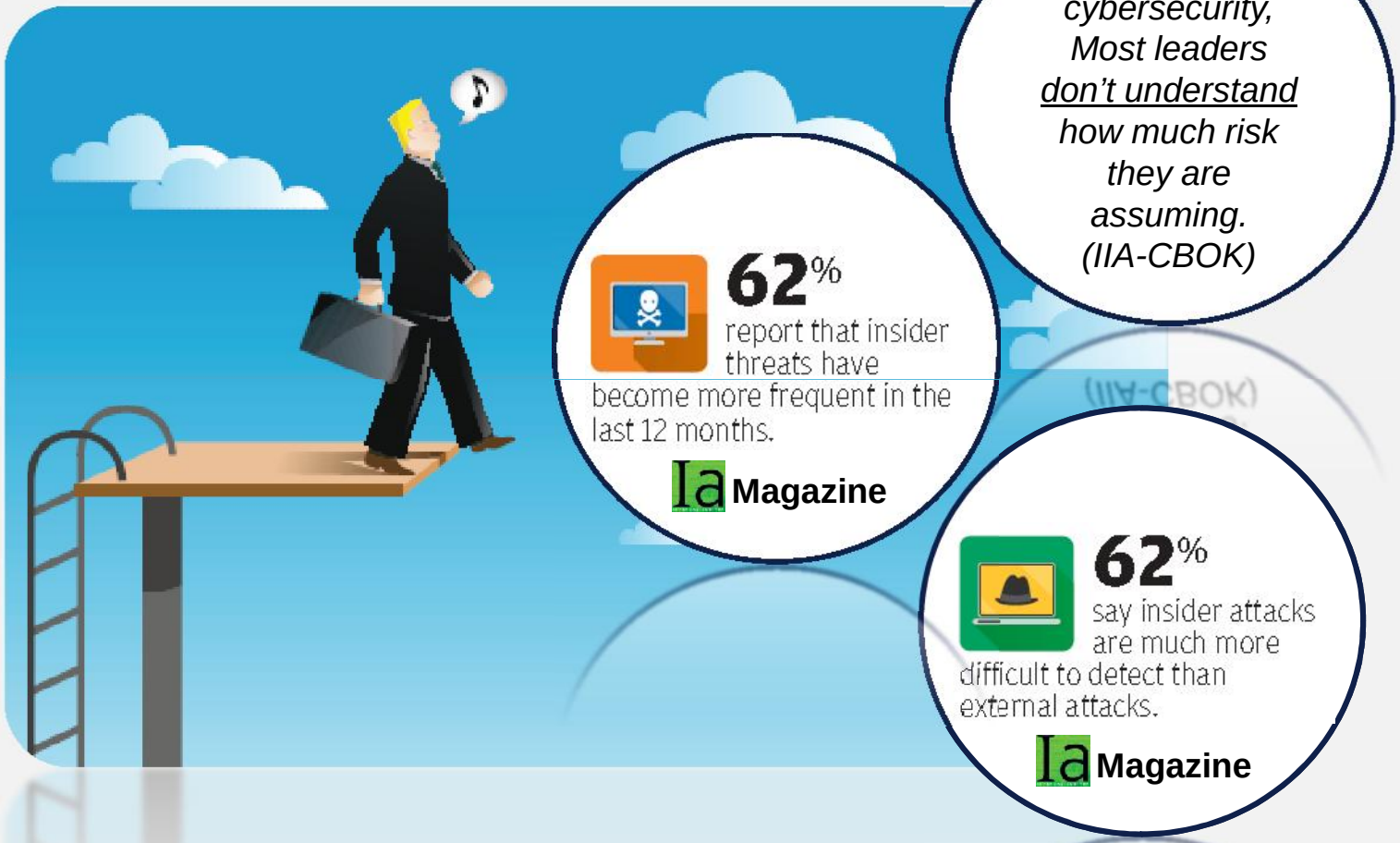


Typical Mobile ApplicationThreats & Vulnerabilities




The People Factor

Understand the Risk



Security is everyone's business (1)

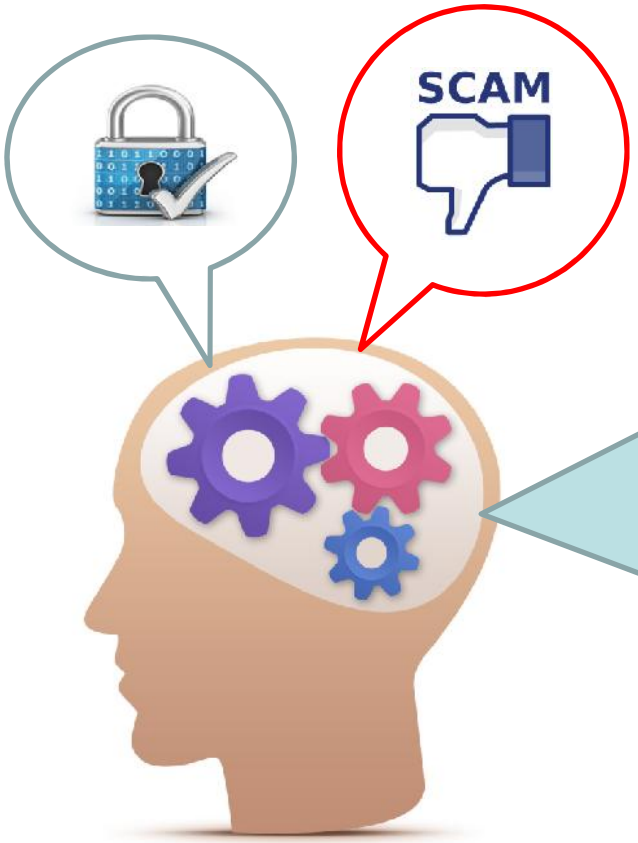
The five principles[2] are:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

IIARF Research Report, IIA & ISACA

SEC_RITY is not complete without 'U'

Scam Savvy Customers



Think before you react. Most spam, viruses and fraudulent emails stress urgency and strongly suggest to take action now—don't become a victim, avoidance of clicking links, responding to unsolicited emails and providing personal information is your defense!

Pausing, Sensing, Avoiding

Security & Compliance Awareness Program

6 Essential Components

Collateral (Newsletter, Blog)

Posters, Desktop Wallpaper

CBT/Online Training & Certification

Events, Seminar & Workshops

Security Intranet Portal

Survey & Behavioral Testing

What about auditors?

52% reported that a lack of cybersecurity expertise among internal audit staff very much or extremely affects internal audit's ability to address cybersecurity risk.

Communicates to executive management and the board the level of risk to the or and efforts to address — 69%

Ensures commu coordination among the organization regarc

Works collaborat and other parties to bu defenses an

Provides assurance ov and response to c — 63%

Ideal: Respondents indicating that internal audit should make significant or extremely significant effort

Actual: Respondents describing their internal audit department as providing significant or extremely significant effort

Internal auditors can play an integral role in the organization to ensure that cybersecurity risks are addressed appropriately, i.e:
(1) extensive audit, (2) verifying the test and simulation made by management

Fraud Data Analytic

Text-Mining → Unstructured Text Data

Speech Recognition → Phone Conversation

Face Recognition → Discrimination Charges

Geo-Tagging → Address Proximity

Web-Mining → Multiple Data Sources

IAIB National Conference - Surabaya 9-10 Nov 2017
ISACA CACS 2017 – Dubai 29-30 Nov 2017

Thank You