
CYBER SECURITY


CYBER
ATTACKS
AHEAD

invincea 2016 CYBERTHREAT DEFENSE REPORT

NORTH AMERICA, EUROPE, ASIA PACIFIC, & LATIN AMERICA

SURVEY DEMOGRAPHICS

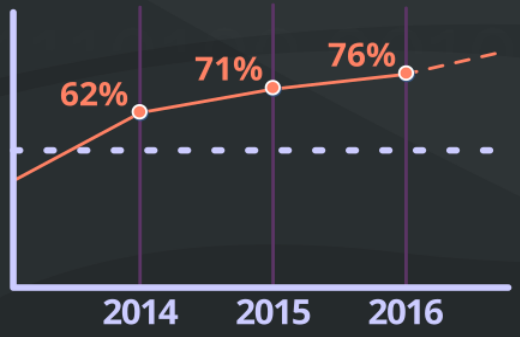
10 Countries represented around the world

20+ Industries represented

1,000 Qualified IT security decision makers & practitioners

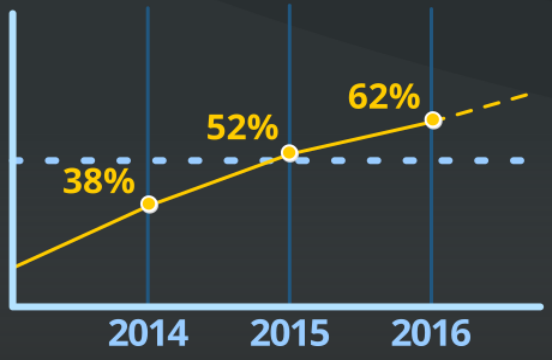
RISING CYBERATTACKS

The percentage of respondents affected by successful attacks is rising each year.



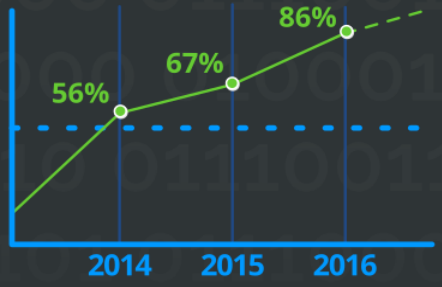
SINKING EXPECTATIONS

Respondents that believe a successful cyberattack is likely in the coming year is skyrocketing.



ENDPOINT PROTECTION REVOLUTION

The percentage of organizations evaluating new endpoint protection solutions to augment or replace their existing investments is skyrocketing.



THE YEAR OF ENDPOINT CONTAINERIZATION

The top four endpoint security technologies targeted for acquisition in 2016 include...

1. CONTAINERIZATION/ MICRO-VIRTUALIZATION
2. SELF-REMEDIATION FOR INFECTED ENDPOINTS
3. DIGITAL FORENSICS/ INCIDENT RESOLUTION
4. DATA LOSS/LEAK PREVENTION (DLP)

SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...

1. LOW SECURITY AWARENESS AMONG EMPLOYEES
2. TOO MUCH DATA TO ANALYZE
3. LACK OF SKILLED PERSONNEL

CYBERTHREAT HEADACHES

Cyberthreats causing the greatest concern include...

1. MALWARE (VIRUSES, WORMS, TROJANS)
2. PHISHING/ SPEAR-PHISHING ATTACKS
3. SSL-ENCRYPTED THREATS

SECURITY'S WEAKEST LINKS

These areas are rated as most difficult to secure...

1. MOBILE DEVICES
2. SOCIAL MEDIA APPLICATIONS
3. LAPTOPS/ NOTEBOOKS

SUSCEPTIBLE NATIONS

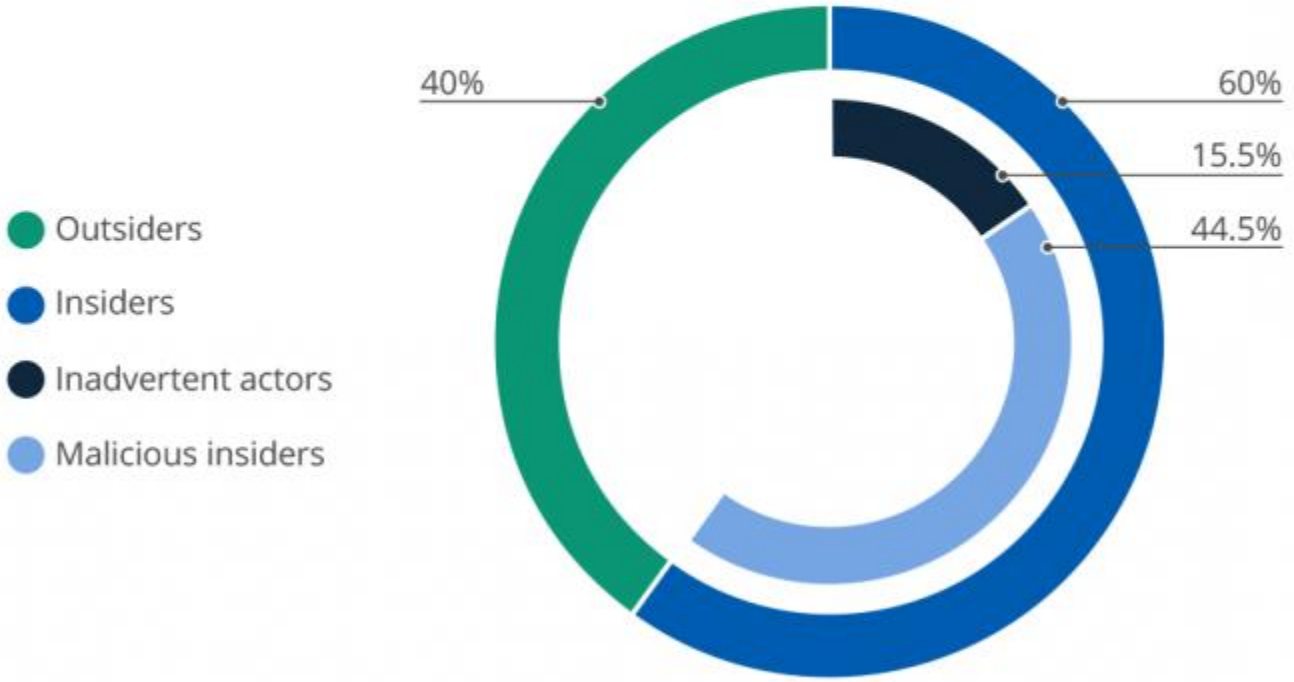
The percentage of respondents affected by successful attacks in 2015 varied by nation.

BRAZIL	89%
FRANCE	82%
CANADA	82%
GERMANY	78%
UNITED STATES	75%
JAPAN	75%
MEXICO	74%
SINGAPORE	73%
UNITED KINGDOM	71%
AUSTRALIA	63%

Tech Chart of the Day

Most Cyber Attacks Are An Inside Job

Cyber attacks by origin of attacker (2015)



BUSINESS INSIDER

Source: IBM

statista


ransomware

ACCOMPLISHMENTS

- All Judicial entities assessed for compliance
  - Plans submitted to achieve full compliance
- All Judicial Entities scanned
- Security Awareness has dramatically increased
- Many vulnerabilities identified and remediated
- Rolling out Comprehensive Security Suite to AJIN customers

LESSONS LEARNED

- Security has been a "Don't Ask, Don't Tell"
- Excessive Reliance on Perimeter Defense
- Too much reliance on EOL technology
- Too little is being invested in maintaining Infrastructure
- Poor Patch Management discipline
- Too little priority has been placed on the activities that secure your environments
- Security vs. Convenience….just ask TSA.
- If you buy it you MUST maintain it……consider the Cloud

MANTRA

Security is NOT a Project.

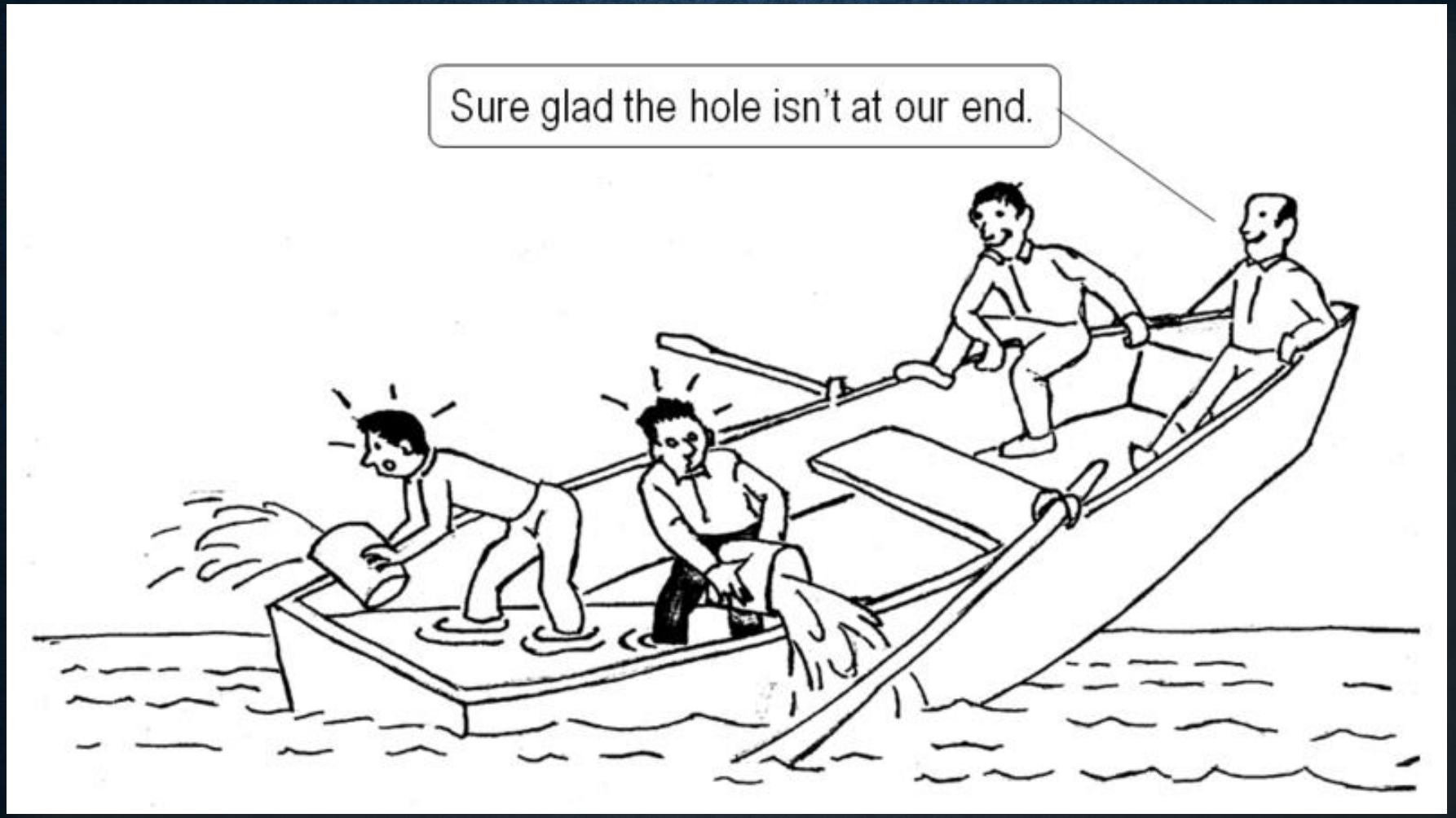
Don't let it become one.

PLANS

- Scan twice per year
- Produce Security Awareness Videos/ training
- Monitor standards compliance
- Monitor Threat Evolution
- Instill Security as a Discipline

MINIMUM SECURITY STANDARD

- Std 2.14
  - File purge for Terminated Employees:
    - Prev: Deletion of folders/files after 4 weeks
    - Proposed: Deletion 6 months after termination
      - Files should be moved offline or moved to more secure storage after 4 weeks.



WE ARE ALL IN THIS TOGETHER