Cyber Financial Crime Summit

Securing the Human – Internal Threats

Educating as a Mitigation Strategy

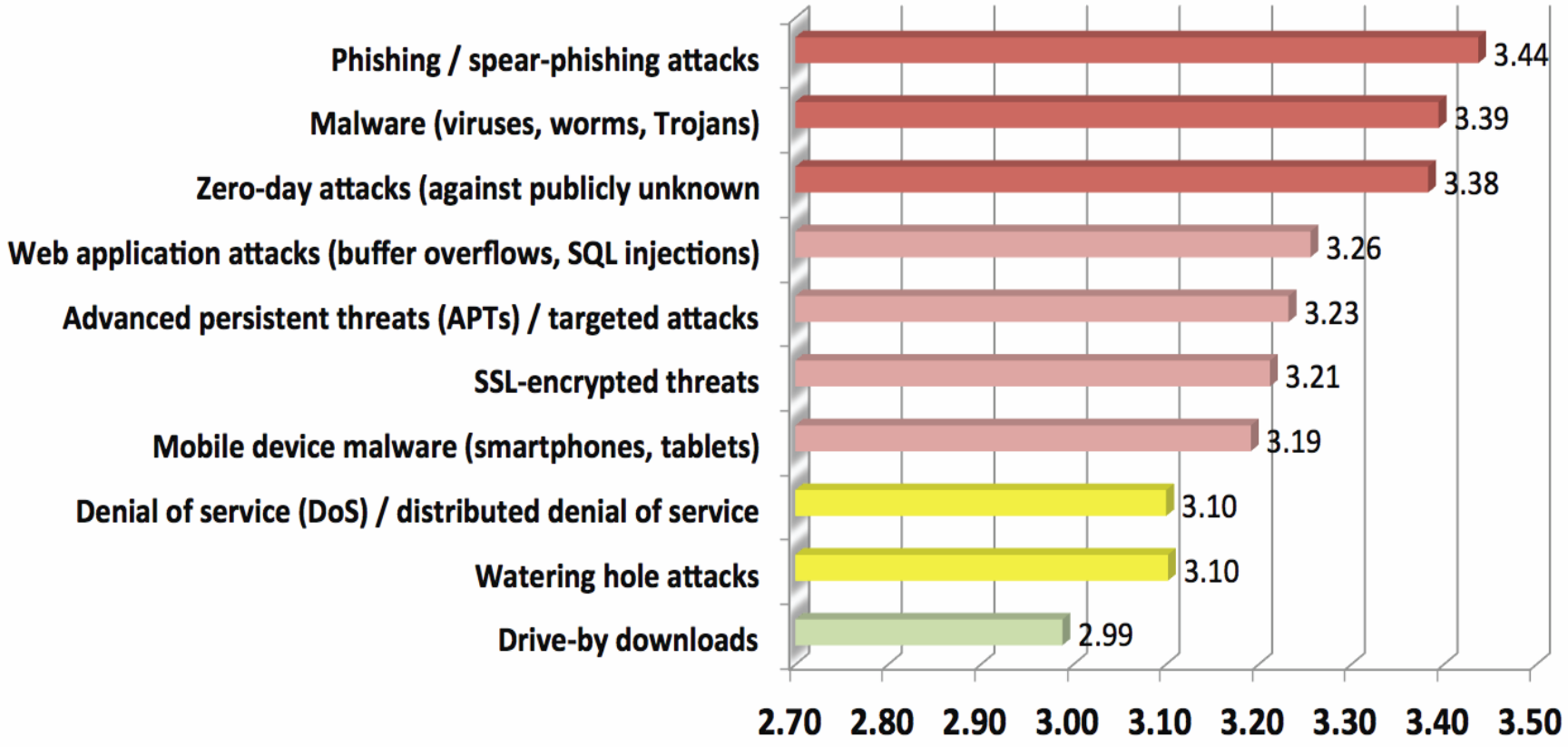
SalientCRGT

Internal Threat Assessment

- Rules of “Least Privilege” must apply to employees
- Anyone can be compromised
- Unintended consequence is still CONSEQUENCE
- Log Files hold the keys to understanding
  - Elevated privileges
  - Data extraction
  - Data exfiltration – sending outside the organization
- Data Classification and Data Loss Prevention

Relative Concern - by type of Cyber Threat*

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (*n=793*)



**A CyberEdge Group Report – 2015 Cyberthreat Defense Report*

Ongoing Security Awareness

- Once a year SAT is not effective
- "Once again, end users represent the most effective means of detecting a breach internally" - Verizon 2012 Data Breach Investigation
- Educate for current threats with appropriate methods
  - Video/Audio clips
  - Cartoons
  - Rewards for valued behavior
- Immediate reinforcement for undesired behavior
  - Phishing
  - Downloads

Takeaways

- Are policies current/consistent with technology controls
- Are appropriate tools functioning as designed
- Does the organization value a security culture
- Is the Security Awareness program up-to-date
- Do Executives “Lead by Example”
- Do users understand their responsibilities
- The Security Chain is only as strong as it’s weakest link and that link is the user
  - Education of the Cyber Warrior is key
    - Who is the Cyber Warrior – every technology user