Cyber Financial Crime Summit

Securing the Human – Internal Threats

Educating as a Mitigation Strategy
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)

- Phishing / spear-phishing attacks: 3.44
- Malware (viruses, worms, Trojans): 3.39
- Zero-day attacks (against publicly unknown): 3.38
- Web application attacks (buffer overflows, SQL injections): 3.26
- Advanced persistent threats (APTs) / targeted attacks: 3.23
- SSL-encrypted threats: 3.21
- Mobile device malware (smartphones, tablets): 3.19
- Denial of service (DoS) / distributed denial of service: 3.10
- Watering hole attacks: 3.10
- Drive-by downloads: 2.99

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