livingsecurity

EXAMPLE. CYBER ESCAPE METRIC RECAP

DECEMBER 2018 | LIVING SECURITY INTELLIGENCE

Context & Insight

Living Security Intelligence assesses thecurrent threat landscape to be one dominated by financially-motivated threat actors, confirmed by recent ransomware and consumer data theft incidents targeting the retail, health service and pharmaceutical industries. These attacks have levied hard costs (i.e. loss of revenue and litigation stemming from breach) and soft costs (i.e. negative publicity and curtailed consumer confidence) against victim organizations.

Moving forward, there will likely be a shift toward espionage-motivated attacks against healthcare and pharmaceutical organizations because of intellectual property holdings, clinical trials and expanded market share. These attacks are highly likely to exploit legacy hardware and/or vulnerable vendors within the supply chain to be successful.

Living Security Intelligence assesses the current human risk profile by documenting the following findings:

- Password-related questions cause the most trouble for employees and likely need clarified by way of additional training
- Risky top-level domains (e.g. .work and .click) appear to be misunderstood by employees
- Employees identified being "caught off guard" as most likely reason to fall for phishing email
- A majority of participants have experienced some type of suspicious-looking email within the last two weeks
- Confidence in spotting phishing emails is slightly elevated compared with actual phishing skills performance (84%)
- Bluejacking and Bluesnarfing attacks may need to be socialized as plausible attacks while traveling or working remotely
- Encryption training may help clarify available options (e.g. FDE)

RISK SCORE

83%

The risk score represents the combined average of education, behavior and policy responses among employees. Results showed an adequate level of security knowledge but a below average policy comprehension (63%), leaving room for improvement.

RECOMMENDATIONS

- Consider clarifying password policy to reduce uncertainty for end users and improve overall policy comprehension
- Increase training on safe online browsing habits to reinforce HTTPS usage and domain awareness
- Ensure least privilege is implemented to limit the number of people who can access sensitive information
- Consider additional training for vendors within the supply chain and/or employees with access to critical assets to improve resilience against espionage-driven attacks
- Balance technical controls with hardening the human perimeter

Contact Us to Experience Game-Changing Security Awareness

livingsecurity.com