

DNS Automation

Arktos Lam – HKIRC

Cybersecurity Manager

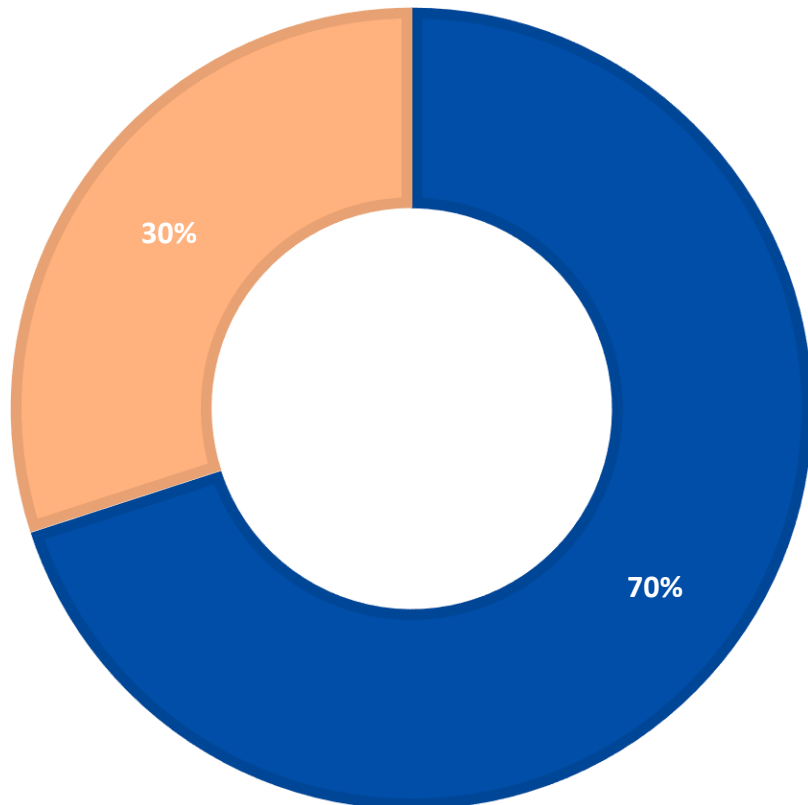


The Disparity in Security Prioritization



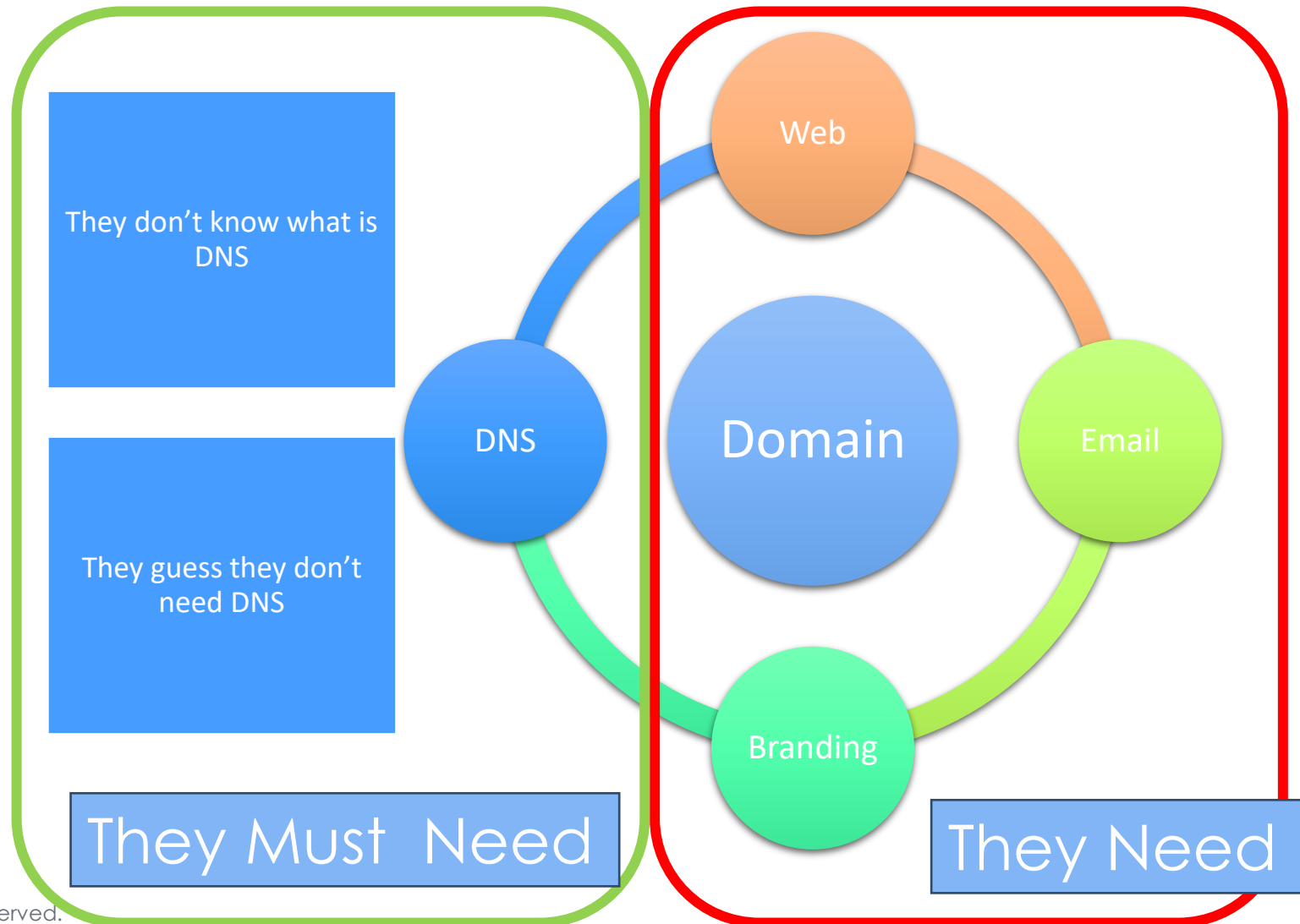
BUDGET SPENDING

■ Web/Email ■ DNS



- High investment in web and email security vs. the minimal cost of DNS security.
- The paradox of DNS: Cheap to maintain but costly when compromised.
- The risk of neglect: DNS attacks can undermine all other security measures.
- discrepancy between spending on web/email security and DNS security.

The Disparity in Security Prioritization



Website

- HTTPS
- WAF
- Vulnerability Scan

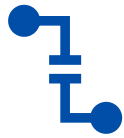
Email

- Anti-Phishing
- Anti-Spam
- Anti-Malware

Branding

- Likely Domain
- SEO

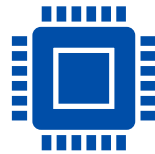
Cybersecurity on DNS



DNS Legacy Protocol:

Built on a foundation of trust, not security.

Lacks security features to cope with modern untrusted networks.



DNSSEC's Mitigating Role:

Introduces security measures to prevent cache poisoning and spoofing.

Protects against DNS-based attacks invisibly.



State of DNSSEC Adoption:

"DNSSEC Ready" signifies available technology and infrastructure.

Implementation and widespread adoption are still limited.



Contrast in Security Visibility:

Security for Email/Web is visible (e.g., HTTPS padlocks, anti-phishing).

DNSSEC works in the background, unnoticed by users but crucial for security.

Accelerating DNSSEC Deployment Like HTTPS?



Brainstorming.

- **User Experience and Perception**
 - **HTTPS Alerts:** Immediate browser warnings for non-HTTPS sites affect user behavior and website reputation.
 - **DNSSEC Visibility:** Lacks direct end-user visibility; not as impactful on user behavior without education.
- **Technical Considerations**
 - **HTTPS Implementation:** Simplified by services like Let's Encrypt; primarily a web server configuration.
 - **DNSSEC Implementation:** Complex coordination required across domain registrars, DNS providers, and site owners.
- **Potential Approach for DNSSEC**
 - **Browser and Resolver Policies:** Warnings or blocks for non-DNSSEC sites could incentivize adoption.
 - **Gradual Enforcement:** Start with recommendations, escalating to stricter enforcement over time.
- **Challenges and Considerations**
 - **Fallback Mechanisms:** DNSSEC failures could unintentionally block access to websites.
 - **Risk of Fragmentation:** Enforcing DNSSEC could lead to inconsistent internet experiences across different resolvers.
- **Conclusion**
 - Enforcing DNSSEC has complex practical implications. A thoughtful, well-communicated approach is vital to maintain an open and accessible internet.

Thanks