ADVANCED PRACTICES COUNCIL® (APC)

CIO Coalition for Open Security

Table of Contents

Executive Summary

The CIO Coalition on Cyber Security (The Coalition) is an assembly of cross industry technology leaders working collaboratively, on a national level, to create a united front in mitigating the risk of cyber-attacks to organizations on both an individual and collective basis. The Coalition believes that the best way to effectively combat ever-increasing cyber threats is through focusing our combined knowledge, resources and efforts to directly target malicious cyber activity. The goal is to identify and implement ways for people, organizations and computers to connect so that collectively we are more intelligent than any single individual, group, or computer.

Purpose

The Coalition's primary purpose is to develop and implement strategies that facilitate cross-industry collaboration to minimize risk from malicious cyber activity.

Objective

To develop shared strategies and constructs resulting in:

- A forum where participants can share any attacks they observe, with appropriate legal and confidentiality protection to encourage reporting without adverse consequences
- The creation of national organization to process and analyze all reported attacks and respond immediately to minimize the threat to national security and disruption of economic activity
- The identification of open source policies, processes and tools for cyber security
- Collaboration between the private, public and non-profit sector security experts
- Challenging the way we address cyber security in our own organizations
- Challenging the way we address cyber security as a community of intelligence professionals
- Partnerships with local, state, and federal agencies dedicated to cyber security
- Collaboration as professionals to understand and solve each other's problems
- The ability to more quickly develop and distribute countermeasures against attacks

Mission Statement

We will create a more secure cyber environment by pooling our individual resources to create a stronger, more proactive, collaborative response to the threats of bad cyber actors.

Keys to Success

- Participation of a critical mass in each of the private, public and non-profit sectors
- Willingness of each member to actively participate in the collaboration efforts defined by The Coalition

- Willingness of all members to openly share their cyber concerns and successes
- Willingness of all members to adopt the collaborative constructs defined and agreed by The Coalition
- Strong engagement and participation from the public sector, including local and federal legislative bodies
- Strong engagement and participation from the PACs in the private sector
- C-Level (C*O) participation from each member company
- The ability of The Coalition to influence the private, public and non-profit sectors to adopt the collaborative constructs defined and agreed by The Coalition
- The ability of The Coalition to influence local and federal legislation
- Communication of risks in a way that triggers constructive action from technology professionals

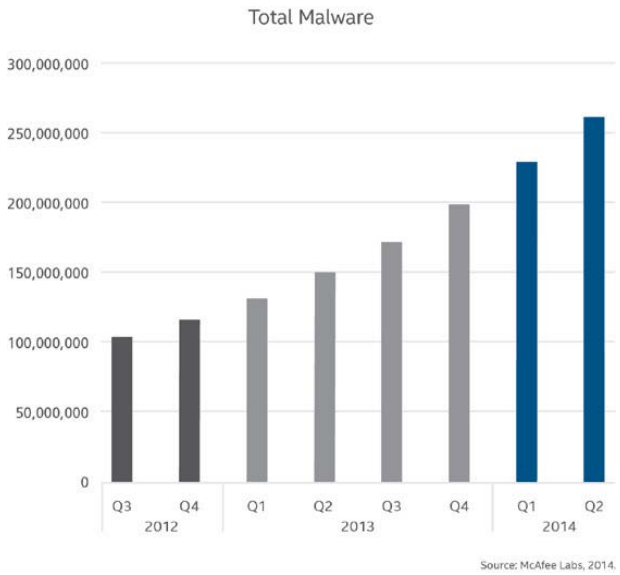
Next Steps

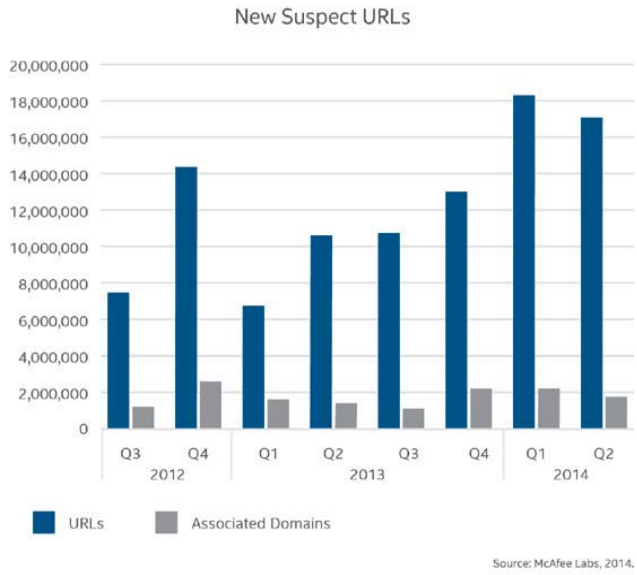
- Identify a leadership board to coordinate the efforts of The Coalition
- Establish a core team to lead this effort
- Identify and solicit broader participation from the three sectors
- Establish a cadence of regular meetings

Background

The types, numbers and frequency of malicious cyber constructs are growing exponentially. These three samples are indicative of a much broader set of cyber threats that every organization and individual must contend with on a regular basis.

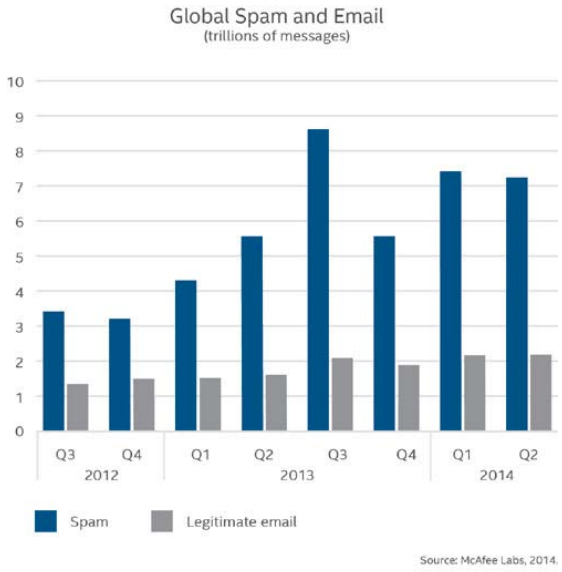
Malware (malicious software) is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is increasing exponentially and is increasingly harder to identify. While prophylactic tools do exist (and are getting better), the bad guys are always ahead of the good guys – requiring constant vigilance.





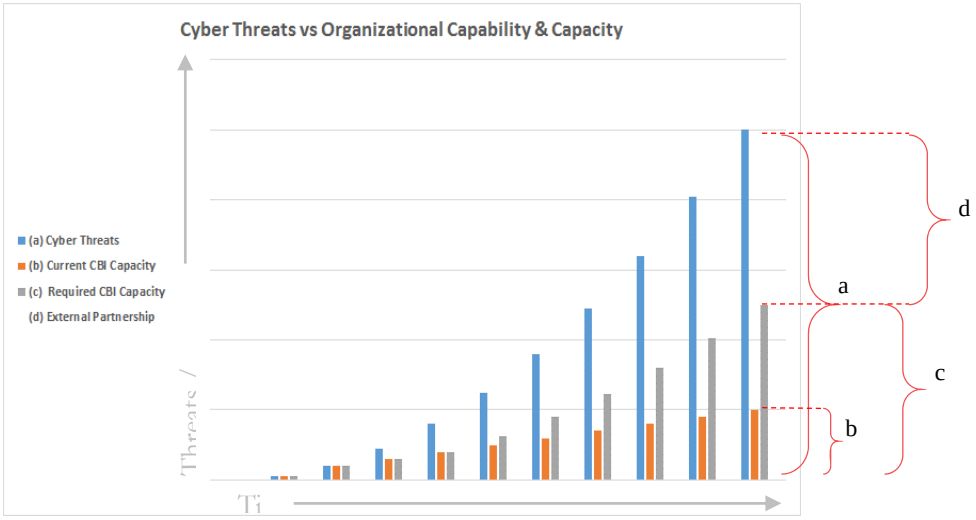
The number of **Suspicious or Known Fraudulent URLs** continues to grow. The quality of these web sites (and the spam that directs the unaware user to them) is getting increasingly better. Even security experts are struggling to easily identify spam and malicious URLs. Vigilance, constant due diligence, and the implementation of state-of-the-art security tools and technologies are table-stakes for today's businesses and include both internal expertise and partnership with external 3rd-party experts to stay current.

Email continues to grow as the primary medium for business correspondence. **Spam emails (unsolicited messages)** represent a significantly larger percentage of overall emails and are often used to introduce malware, direct individuals to suspect or malicious URL's, and serve as the primary medium for phishing (an e-mail fraud attempt seeking unauthorized access). Constant monitoring and education regarding the ever-shifting threats introduced via spam are critical to protecting our organizations and people.



While cyber threats are growing at an exponential rate **(a)** and cybersecurity ***awareness*** is growing, most organizations have yet to progress their ***cybersecurity maturity*** to combat this threat.

Many organization have made small changes **(b)** to increase focus on cybersecurity. However, most organizations continue to lag behind the bad actors and recognize that there is an urgency to up-weight their internal and external cybersecurity capabilities.



With that in mind, many organizations are evaluating their cybersecurity requirements against their current security organization and may need to up-weight their internal cybersecurity teams **(c)** and will still need to supplement their teams with external security partners **(d)** to ensure they remain current and compliant as they protect their people and organization's information assets.

The Society for Information Management – Advanced Practices Council (APC) has identified an opportunity to supplement both our internal and external cybersecurity teams by coming together to share in our challenges and successes and collectively fight the cyberwar in the formation of The CIO Coalition for Open Security.