2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Mission Statement

This program enables intelligence community analysts and private sector partners to gain a greater understanding of how their disparate, yet complementary roles can work in tandem to ensure mission success.

Developed with
The views and opinions expressed in this document do not necessarily state or reflect those of the U.S. Government or the Exchange Program Partners, and they may not be used for advertising or product endorsement purposes.

This document is provided for educational and informational purposes only and is not intended and should not be construed to be a warranty, guarantee, or representation regarding the accuracy, completeness, or usefulness of any information, apparatus, product, or process discussed in this document. U.S. Government and Exchange Program Partners do not make any representation or warranty, express or implied, regarding the accuracy, completeness, or usefulness of any information, apparatus, product, or process discussed in this document. The views and opinions expressed in this document are those of the authors, and do not necessarily reflect those of the U.S. Government or the Exchange Program Partners, and may not be used for advertising or product endorsement purposes.

60%
of SMBs will close within six months of a cyber-attack.
of cyber-attacks target SMBs.

— National Cyber Security Alliance, 2016

Cyber Threat Recognition and Mitigation Group Contributors

AMS
Hewlett Packard Enterprise
Stratus Cyber
Small Business Security
iX
America Cyber Solution
Small businesses must prepare for cyber-attack. The first three steps to prepare for a cyber-attack on your business involve PEOPLE, SYSTEMS, and BACK-UPS.

Step one, PEOPLE. Educate employees about the threat, starting with use of strong passwords and learning about threats like phishing.

Step two, SYSTEMS. Protect your systems and data by using some of the many software tools available, starting with Anti-Virus and a Firewall.

Step three, BACK-UPS. Give you a do-over, after an attack instead of going out of business, it allows you to start again from where you left off.

Some of the most affordable yet effective prevention techniques that SMBs can employ to prevent cyber-security breaches include: firewalls, intrusion prevention software and Anti-Virus software, strong passwords with expiration timers, disabling and uninstalling any unused services and software, application whitelisting/black listing and physical access controls (e.g. locked doors, offices, cabinets).

Software should also be patched with the latest vendor releases so that known security flaws are closed.

You've been hacked, you've responded appropriately to the incident and now you need to recover. The extent of your recovery may include the computer room and environment, the hardware, connectivity to a Internet Service Provider (ISP), software applications, and restoration of your company’s data.

Help from your ISP, hardware vendor, trade associations or major clients may be available. A number of helpful ideas can be found on the Federal Trade Commission (FTC) and other official websites. If you have not yet created an incident response plan, consider consulting with professionals. If you have not yet created a disaster recovery plan, consider consulting with professionals.

Consider using a managed security service provider to monitor your network for advanced persistent threats. An endpoint security solution will provide additional security for your endpoints (laptops, workstations, servers). This defense-in-depth strategy enhances the security tools and best-practices in your prevention strategy.

Your diligence is critical! Familiarize yourself with the signs and symptoms of an infected system. Use security resources and information channels to keep current on emerging threats and security updates. Keep the contact information of security service providers that manage your security, and identify other professionals that you can call to help you recognize and respond to security incidents and breaches.

The estimated average cost of a data breach for healthcare organizations is $2.2 MILLION — Benchmark Study on Privacy and Security of Healthcare Data (6th Annual) — MTrends 2016

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach

The median number of days an organization was compromised in 2015 before the organization discovered the breach