CYBERTHREAT | RECOGNITION & MITIGATION

A GUIDE FOR SMALL & MEDIUM SIZED BUSINESSES (SMBs)

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.

Cyber Threat Recognition and Mitigation Group Contributors

AMGEN · Hewlett Packard Enterprise · StratusCyber Small Business Security · TAX Virginia Department of Taxation · Armera Cyber Solutions

Developed with TRUDEAU | CREATIVE

This document is provided for educational and informational purposes only and is not intended and should not be construed as providing legal advice. U.S. Government and the IC Private Sector Public Sector Analyst exchange program partners (the "Exchange Program Partners") do not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process discussed in this document. U.S. Government and the Exchange Program Partners do not endorse or recommend any commercial products, processes, or services. 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.

CYBERTHREAT | RECOGNITION & MITIGATION

A GUIDE FOR SMALL & MEDIUM SIZED BUSINESSES (SMBs)

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

of cyber-attacks target SMBs.

— National Cyber Security Alliance, 2016

YOUR PATH TO IMPROVED CYBERSECURITY

1 PREPARE 2 PREVENT 3 DETECT 4 RESPOND 5 RECOVER

1 PREPARE

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.

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

NO SHORTCUTS IN YOUR PREPARATION

5 RECOVER

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 Ready.gov, NIST, SBA and other official websites. If you have not yet created one, a disaster contingency planning policy or reference book can be crucial in times of crisis.

2 PREVENT

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 to limit entry points into the system, 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.

3 DETECT

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.

4 RESPOND

When an incident is detected, it is important to respond thoroughly and timely. Work with pre-established contacts to contain, mitigate, and eradicate the threat.

Affected parties should be alerted and provided with progress reports throughout the incident. Ensure all the attacker's artifacts are eliminated from affected systems, determine cause and symptoms of the incident, patch all vulnerabilities, and restore data appropriately from backups.

Try to preserve evidence so law enforcement action can potentially be taken against the perpetrator.

146

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

— MTrends 2016

$2.2 MILLION

The estimated average cost of a data breach for healthcare organizations

— Benchmark Study on Privacy and Security of Healthcare Data (6th Annual)

430 MILLION

New unique pieces of malware discovered in 2015, up 36 percent from the year before

— Symantec Internet Security Threat Report 2016

CYBERTHREAT | RECOGNITION & MITIGATION

A GUIDE FOR SMALL & MEDIUM SIZED BUSINESSES (SMBs)