CYBERTIPS

HED: Ten Cybersecurity Myths Busted
Deck: And the Top Ten Network Security Best Practices to Better Manage Risks

Government IT organizations are under increasing intense pressure to consolidate IT operations and refine cybersecurity initiatives to balance the need to cut costs, against requirements to better manage security and associated risks. This delicate balancing act is forcing many public sector organizations to make difficult decisions that must be carefully weighed. The following is a list of top cybersecurity myths that agencies must 'bust' to achieve greater security, and better manage ongoing risks.

1) Complying with FISMA (along with other mandated federal security regulations) guarantees cybersecurity protection.
--BUSTED--
Not true. Complying with current federal security regulations does not guarantee an agency's IT operations and resources are adequately protected against breaches or other forms of intrusion -- from either external threats or the inappropriate actions of internal audiences. Adhering to regulations, and reporting to federal oversight organizations is an ongoing requirement that must be weighed against the level of security actually required, as well as the budget available to protect agency information resources. Agencies must shift away from point solutions and strive to develop a strategic cyber security program to better protect their operations and limit the scope of any intrusions on networks. That program must also incorporate a functional recovery plan.

2) Restricting or disallowing the use of personal mobile devices will protect government resources.
--BUSTED--
Unrealistic. The influx of mobile devices is a reality agencies must somehow learn to embrace. Restricting or disallowing the use of personal mobile devices by employees will grow increasingly difficult, and may negatively impact productivity and hiring prospects for those organizations. A better solution is to invest in centralized client computing alternatives such as client virtualization, to better manage and control access to agency information resources and secure users no matter where they are located on any given day.

3) The more restrictive the policy, the better protected the organization's resources.
--BUSTED--
Again, not true. Organizations with the most restrictive security policies must work to better incorporate the needs of agency personnel and other stakeholders to access information. Policy is one part of a comprehensive cyber protection strategy, but should be thought of as a way to keep honest people honest. What the organization really should do instead is focus on keeping dishonest or disreputable people from gaining access to agency networks and information resources. Reliance upon an assured network, one that is trusted, reliable and secure, is a much more effective way to protect the organization's information resources.

4) Cloud services, especially public cloud services, are not to be trusted.
—Soon to be BUSTED--
Not always true. The continual evolution of cloud-based services is helping to vastly improve the security measures of providers who are delivering access to government resources. In many cases, even public cloud services have now grown to be more secure than traditional physical network infrastructures used

by government agencies today. This trend will continue as the desire for trusted cloud applications drives increasingly robust user authentication, authorization and protection mechanisms.

5) "Minimizing the attack surface" of a government organization by consolidating access to web sites and network resources will allow an agency to achieve full protection against security breaches.
--BUSTED--
Not true. Minimizing the attack surface indeed helps to reduce access points to government networks and information. But this alone won't protect agencies against other forms of breaches, such as breaking into the physical network media. Several factors enable an agency to attain full protection, including consideration of the scope of damage likely to occur if a break-in takes place, along with how best to recover from an attack. In the event an intruder successfully gains access to the network, there should be enclaves established that limit that intruder's ability to defeat the entire network. It's better to have a partial outage, in one geographic or functional area, rather than to lose the operational functionality of the entire network. There's also a requirement to quickly recover from outages, whether caused maliciously or accidentally. All of this can be accomplished through an assured network design that utilizes technologies such as virtualized switching architectures, redundant path routing in a mesh network and bulk encryption of network traffic.

6) Maintaining a traditional physical networking infrastructure is the best way to avoid breaches.
--BUSTED--
Not true. Traditional infrastructures are not inherently more secure than other modern IT operational environments. In fact, depending on the age and the level of ongoing maintenance employed/required to maintain operations now, it's increasingly clear that aging network infrastructures can pose unacceptable levels of risk.

7) Funding isn't necessary to improve security protections, only tighter/more restrictive policies, are required, instead.
--BUSTED--
Not true. There's no easy way to achieve an acceptable level of risk through administrative mandates. Policies alone won't resolve an agency's ongoing challenge in balancing requirements for security against the growing need for greater access, transparency and accountability. Agencies must find new ways to invest smartly in systems that allow them to protect internal information resources, while also enabling operational efficiencies and broader accessibility.

8) Using a firewall and antivirus tools will protect agency resources.
--BUSTED—
Not true. Firewalls and antivirus protections won't protect against any conceivable attack. Increasingly, government organizations have found that it takes a strategic approach to security to assure protection of IT resources. That approach will vary depending upon the information in question, the network architecture and the agency's resources. One example would be to include bulk line rate encryption, along with firewalls and antivirus tools, for the 'sensitive enclaves' of an agency's infrastructure.

9) Ignoring/overruling traditional cybersecurity policies to enable greater collaboration will allow greater information sharing, and increase productivity, and won't increase an agency's risk of a security breach, or other intrusion (or at least not that much).
--BUSTED--

Not likely. Agencies that have gone against federal regulatory policies to enable greater productivity and access to information have also had to simultaneously invest in more modernized security mechanisms. There are numerous tools and services available to allow workers to safely continue to share information and resources no matter where they are located. But agencies must first take the time to perform a proper full-scale assessment of current operations, procedures and security requirements to enable flexible, yet secured access to information and network resources.

10) Sidestepping investments in backup and recovery are 'a manageable risk' during this difficult budgetary time.

--BUSTED--

Not true. Continuity of Operations Planning (COOP) requirements vary depending on the agency's operational requirements and the classification levels of information housed on agency networks. There's no excuse for not properly protecting government data that has been properly classified, based on its ongoing storage and recovery requirements. Use of emerging cloud-based data center backup solutions only further de-bunks this myth. There simply is little reason to allow government information resources to go unprotected.

-end-