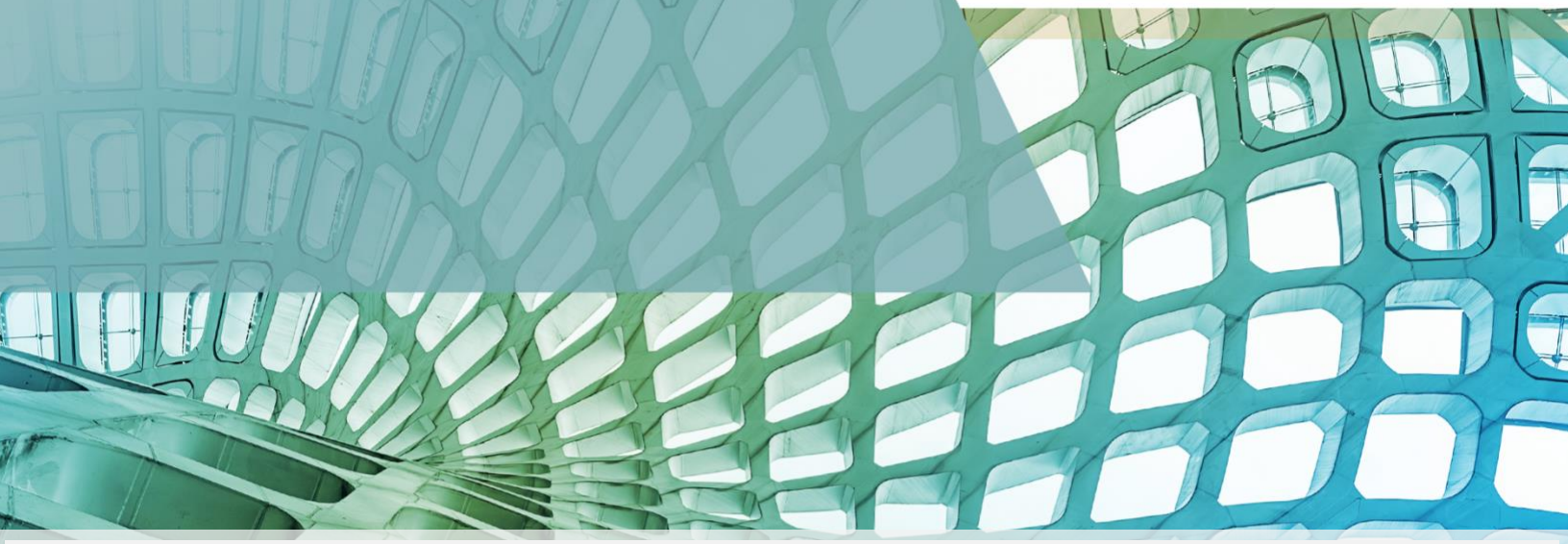
NXTKey



White Paper - Top 10 Cyber Security Needs in US Federal Government 2018

PROACTIVE SECURITY
CYBER MANAGEMENT SERVICES
SECURITY OPERATIONS CENTER (SOC)
SECURITY ARCHITECTURE & ENGINEERING

www.nxtkey.com

Federal agencies, as well as critical infrastructures such as communications, transportation, energy, and financial services, are all highly dependent upon computerized (or cyber) information systems, as well as electronic data, for carrying out their operations.

The ability to process, maintain, and report information is also dependent in large part on cyber operations. Because of this, our everyday lives, along with economic vitality and national security rely heavily upon a safe, stable, and resilient cyberspace.

Unfortunately, though, cyberspace - as well as its underlying infrastructure - are becoming more vulnerable every day to a wide array of risks. Such risks can stem from both physical and cyber-related threats.

In fact today, there are a whole host of cyber actors that can quickly and easily (and oftentimes, silently) exploit cyber vulnerabilities in order to steal information and / or to destroy, disrupt, or threaten the delivery of essential services.

Cyber Security Vulnerabilities in Federal Government

Based on information from the 2017 Presidential Order on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure, "Known unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies."

Just some of the many known vulnerabilities can include the following:

- Using operating systems or hardware beyond the vendor's support lifecycle
- Declining to implement a vendor's security patch
- Failing to execute security-specific configuration guidance

There are numerous cyber threats that can befall the Federal government, as well as its citizens. With that in mind, the top cyber security services needs of the Federal government include the following:

1) Support to Critical Infrastructure

Cyber attacks are increasingly becoming more dangerous, and more targeted. Such attacks can go far beyond just simply hacking into the computer systems of individuals and businesses. In fact, many threats are designed by advanced actors with the purpose of damaging and / or disrupting critical U.S. infrastructure that deliver vital services such as electricity and financial services.

Attackers can inflict a great deal of damage on physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services - even without an actual physical attack.

Cyber threats today are actually two-fold. These can include attacks that target information technology (IT) - which includes the software and networks that underpin business functions in critical sectors such as financial services. It also can include attacks that target operational technology (OT) - which includes control systems that are designed for operating physical processes such as power flows in the electrical grid.

Should such an attack occur, even backup networks could quickly become flooded and unreliable in the event of disruption of primary communications like phone and cell communications, and Internet / email. Therefore, an attack on critical infrastructure could in turn present a national security challenge unlike any other.

Today, a cyber attack can essentially deliver the same damage and / or consequences as a kinetic attack. And, because cyber and physical security are interdependent, ensuring the safety of both must be a core aspect of the risk management strategies and services.

2) Resilience Against Botnets and Other Automated, Distributed Threats

A botnet typically operates without obvious visible evidence, and can remain operational for many years. This "robot network" can be used in many ways, including for DDoS (distributed denial of service) attacks and spam services, malware distribution, and other organized criminal activity.

Likewise, botnets could also be used for covert intelligence collection - and terrorists or state-sponsored actors could even use a botnet for attacking Internet-connected critical infrastructure.

3) Disruption of Electricity and Other Necessary Utilities

With utilities in the United States - and around the world - increasingly moving towards smart grid technology (as well as other upgrades that possess inherent cyber vulnerabilities), correlative threats from malicious cyber attacks on the North American electric grid continue to grow, both in sophistication and in frequency.

Nation states such as China, Russia, and Iran - as well as non-state actors, which include foreign terrorist and hacktivist groups - can pose varying threats to the U.S. power grid. In fact, a determined, well-funded, and capable threat actor with the appropriate attack vector can succeed to varying levels, depending on what type(s) of defenses are in place.

Given this threat, the Federal government should be better able to determine when and where such attacks may occur so as to reduce - or possibly even eliminate - threat to the country and its citizens.

4) Securing Federal Networks

The federal enterprise depends largely on information technology (IT) systems, as well as computer networks, for many of its essential operations. These systems, however, are facing large and diverse cyber threats, which can range from unsophisticated hackers to technically competent intruders that use high-end, state-of-the-art techniques.

Many of these malicious cyber attacks are designed for stealing confidential information, as well as for disrupting, denying access to, degrading, and / or for destroying critical information systems.

5) Privacy Protection

Just as with individuals and businesses, the Federal government faces many privacy protection issues when it comes to cyber security. While regulations have been passed - such as the Cybersecurity Information Sharing Act of 2015 - many industry experts state that much more still needs to be done in order to increase both the quality and the quantity of information that is being conveyed to and from government entities, as well as to and from private sector officials.

6) Cyber Economic Crime

As more of global economic activity is moving to the cloud, the threat of cyber economic crime will also continue to grow. One reason for this is because this type of crime is less dependent upon human interaction, as well as the fact that it can be performed by individuals who are either inside or outside of a country's borders. There are several types of cyber economic crimes that have topped the list over the past few years. These include bribery, procurement fraud, and asset misappropriation.

7) Digital Theft of Intellectual Property

Intellectual property theft involves robbing people or companies of their ideas, inventions, and creative expressions - known as "intellectual property" - which can include everything from trade secrets and proprietary products and parts to movies, music, and software.

But this type of theft is not just limited to individuals and businesses, but can also occur with government entities - and it is a growing threat, particularly in light of the rise of digital technology and Internet file-sharing networks.

Preventing intellectual property theft is a key priority of the United States Federal Bureau of Investigation, or FBI's, criminal investigative program. It focuses in large part on the theft of trade secrets and infringements on products that can impact consumers' health and safety, such as counterfeit aircraft, vehicle, and electronic parts.

In fact, the FBI participates in the U.S. Immigration and Customs Enforcement's Homeland Security Investigations-led National Intellectual Property Rights Coordination Center (NIPRCC) - which stands at the forefront of the U.S. Government's response to global intellectual property theft and enforcement of its international trade laws.

8) Illicit E-Commerce (Including Hidden Marketplaces)

Another cyber security service need of the Federal government entails that of dealing with illicit e-commerce - including "hidden" marketplaces. This is oftentimes referred to as the "darknet" market, which involves the running of a commercial website, and deals in black markets such as the selling or brokering of drugs, cyber-arms, weapons, counterfeit currency, stolen credit card information, forged documents, unlicensed pharmaceuticals, and other illicit goods.

9) Internet-Facilitated Proliferation of Arms and Strategic Technology

Ever since the 9/11 attacks on the United States, the U.S. Citizenship and Immigration Services (USCIS), via its enforcement unit (the ICE, or Immigration and Customs Enforcement), has used its skills to hunt for terrorists. The mission of the department's Cyber Crimes Center is to investigate both domestic and international criminal activities that occur on, or are facilitated by, the Internet.

Terrorists often make use of the Internet for finding the means and the methods of conducting business, sharing information, and issuing instructions. The ICE's Arms and Strategic Technology division looks to prevent the proliferation of weapons, as well as the movement of terrorists and other criminals from entering the United States.

But there is still a growing need for additional services in this area. For example, falsified passports can be a particular problem for the USCIS, as the range and the design can depend upon the country of issue.

10) Cyber-Enabled Smuggling and Money Laundering

Likewise, the United States' ICE division also distinguishes itself in the area of illegal arms and money laundering. For instance, unlike the more "traditional" methods of money laundering - which rely on the banking system - cyber money laundering depends more on the use of various types of transactions and financial services providers, which can range from wire transfers, cash deposits and withdrawals and e-money transactions, to "money mules" and remittance services.

The choice of tools and mechanisms that are used by criminals to launder cybercrime proceeds can be quite diverse. However, some of the more common of these include the following:

- Use of accounts that are opened with the help of lost documents or nominees;
- Use of fictitious (transit) companies;
- Use of remote access to carry out financial transactions via multiple bank accounts;
- Use of cash in the final stage of the chain of financial transactions;
- Use of alternative payment systems (such as e-payments), both national and international;
- Purchase of electronic money and use of e-wallets;
- Conversion of illegal proceeds into goods through the purchase of the latter via the Internet.

Conversion of stolen funds into cash is common because the movement of cash outside of the banking system is nearly impossible to track. Therefore, the need for higher levels of security are also necessary in this area cyber crime.

Strategies for Effective Cyber Risk Management

Today's world is more interconnected than ever before. However, even with all of the speed, convenience, and array of other benefits that this connectivity can bring, it also brings about the increased risk of fraud, theft, and abuse - and because of that, individuals, businesses, and governments have become much more vulnerable to cyber attacks.

The United States Department of Homeland Security works with other federal agencies in conducting high-impact criminal investigations for the purpose of disrupting and defeating cyber criminals. This tremendous task is only growing, though.

According to the 2017 Presidential Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, "Cybersecurity risk management comprises the full range of activities undertaken in order to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents."

The report goes on to state that, "Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity."

Cyber criminal threats pose very real risks to both the economic security and privacy of the United States, its government, and its citizens. With that in mind, both criminal investigators and experts in the area of network security are working - and using available tools - in order to effectively investigate and respond to cyber incidents. However, as the need for cyber protection continues to grow, the effectiveness of available tools must also expand in order to meet cyber security requirements.

About the Author:

Shivaji Sengupta is a seasoned business management and solutions development entrepreneur who has over 24 years of experience providing solutions to customers across 17+ countries in the areas of cyber security, enterprise information management, content management and information technology.

Mr. Sengupta's company NXTKey Corporation provides cyber security solutions to key federal government agencies supporting them in maintaining their cyber defensive posture. Mr. Sengupta is also an Adjunct Professor for Cyber Security at Delaware State University. He has designed and is teaching the Applied Cyber Security Course at DSU.

About the Company:

NXTKey Corporation is an agile Small Business that places emphasis on teamwork and partnership with our clients to produce optimum contract performance. We have refined our solution from experience supporting highly complex Department of Justice (DOJ) environments such as United States Marshals Service (USMS), Justice Management Division (JMD), Office of Justice Programs (OJP) and Federal Prison Industries (FPI).

Our depth of experience allows us to provide IT security support for a wide range of IT General Support Systems (GSS) and major applications (MAs) within the Federal Enterprise and following the guidance in the Federal Enterprise Architecture (FEA) and information systems security support services in accordance with OMB Circular A-130, NIST guidelines and standards, as well as other federal policies and regulations.

We specialize in providing our clients a full range of security services specifically tailored to their requirements. These services include: Certification & Accreditation, Security Architecture, Mobile Security and Governance, Risk Analysis and Assessments, Security Policy and Processes, System Auditing, Security Control Assessment, Disaster Recovery Planning, Contingency Planning, Vulnerability Assessment, Penetration Testing, Physical Security Survey, Information Systems Security Training and Security Program Management.

More information on our website at https://www.nxtkey.com