eGUIDE

OneNeck IT SOLUTIONS *a TDS® Company*

presents

State & Local Government Cybersecurity

In recent years, cybersecurity has become the number one priority for state and local government CIOs. Achieving and maintaining cybersecurity is an ongoing and necessary imperative. Yet, protecting government information and citizens' personal data has become more challenging as networks and the amount of data on them has grown exponentially.

All organizations must rethink their security practices and ensure that they are following a holistic strategy throughout the enterprise to secure sensitive data.

We offer this eGuide as insight to how emerging threats may affect your IT infrastructure and key strategies for defense.

Read more...

The Threat Landscape

Cyber-attacks continue to evolve in scope and sophistication – it's much larger than hacking and data breaches.

Research firm MarketsandMarkets foresees the cybersecurity market growing from $122.45 billion in 2016 to $202.36 billion in 2021. The cost of data breaches is estimated to rise to more than $2 trillion by 2019, and the onslaught of IoT devices is expected to muddle the threat landscape. By 2020, a quarter of identified enterprise attacks will involve internet-connected devices, according to Gartner.

While scale and scope vary, attacks fall into **one of the following five categories.**

1. Network and Application Layer Attacks

Application layer attacks are the hardest to defend against, because this is the layer that is most exposed. These attacks result in a suspension of internet-connected server and network resources. Exploit kits, readily available on the black market, make these attacks easy to launch and difficult for companies to resolve. There are many different methods — here a just a few:

- **Denial of service (DDoS) —** This attack targets either the application layer or the network layer where traffic floods the network to prevent authorized users from accessing information or services.

  - Network level: Malicious packets are sent over many different network protocols to clog the pipes to consume the bandwidth and prevent access to the target.

  - Application level: Also known as an HTTP flood, consumes a Web server's CPU and RAM to deny legitimate clients from accessing the server.

- **Brute Force —** Passwords, session identifiers, directories and credit cards are deciphered through trial and error to determine an unknown value by using an automated process. This attack underlines the importance of using complicated passwords and two-factor authentication.

- **Secure Socket Layer (SSL) Attacks —** Attacks with names like Lucky 13, RC4 Cipher, Heartbleed, POODLE, Shellshock and FREAK work to decrypt protected browser cookies and encrypted SSL communications.

2. Social Engineering

Social engineering relies on human emotion and error rather than technical vulnerabilities. A user is sent a fake email or other communication that tricks them into submitting passwords or personal information. As the source appears to be legitimate, this attack is hard to detect. Phishing is a prevalent form of social engineering; users may be tricked into submitting sensitive information, by pretending to need to verify bank data, threatening legal consequences, or offering a time-sensitive offer. This very useful technique may place critical enterprise information into malicious hands.

3. Advanced Persistent Threats (APT)

APT involves any breach where the attacker infiltrates the network and remains undetected for as long as it takes to escalate privileges and steal sensitive data. Connections may initially be made through phishing or social engineering schemes to create a backdoor access, which allows hackers the ability to stay inside the network for a long time. It can be weeks or months, or even years, before the breach is detected, and sometimes is only discovered when conducting an audit.

4. Cybercrime Syndicates

Organized cybercrime is on the rise. According to a McAfee report, there are an estimated 20 to 30 cybercrime syndicates with nation-state level capabilities operating in Russia alone. These syndicates offer hacking-as-a-service, such as the widespread use of malicious software to steal credit card information and sell it on the black market. Kits available on the dark web allow hackers with even low-level skills to launch a ransomware attack or other malware.

5. Major Data Breaches

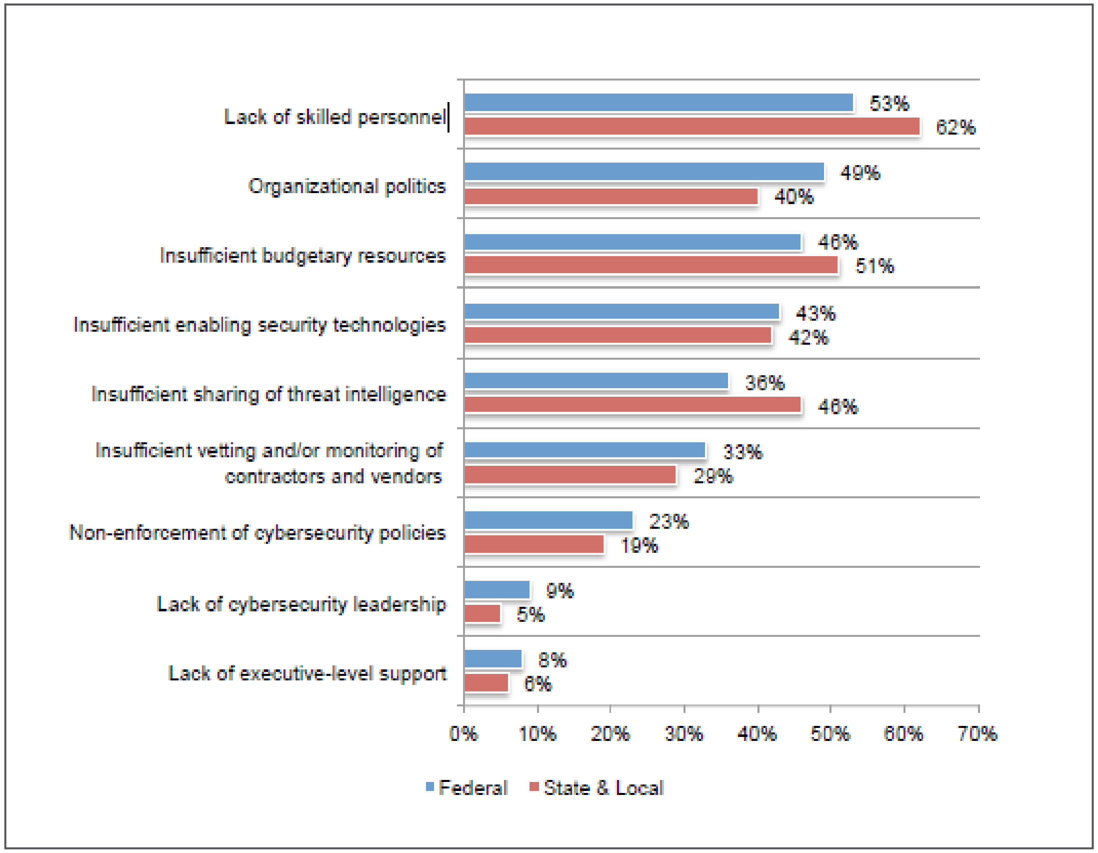
A major data breach may have employed a number of tactics used to infiltrate a network and extract vast amounts of sensitive data with the intent to expose, disrupt operations or bring down an entire company. The 2015 cyber-attack on Anthem health insurance is a great example, where 80 million records containing income, social security and addresses of current and former patients and employees were compromised.

Why are state and local governments so vulnerable?

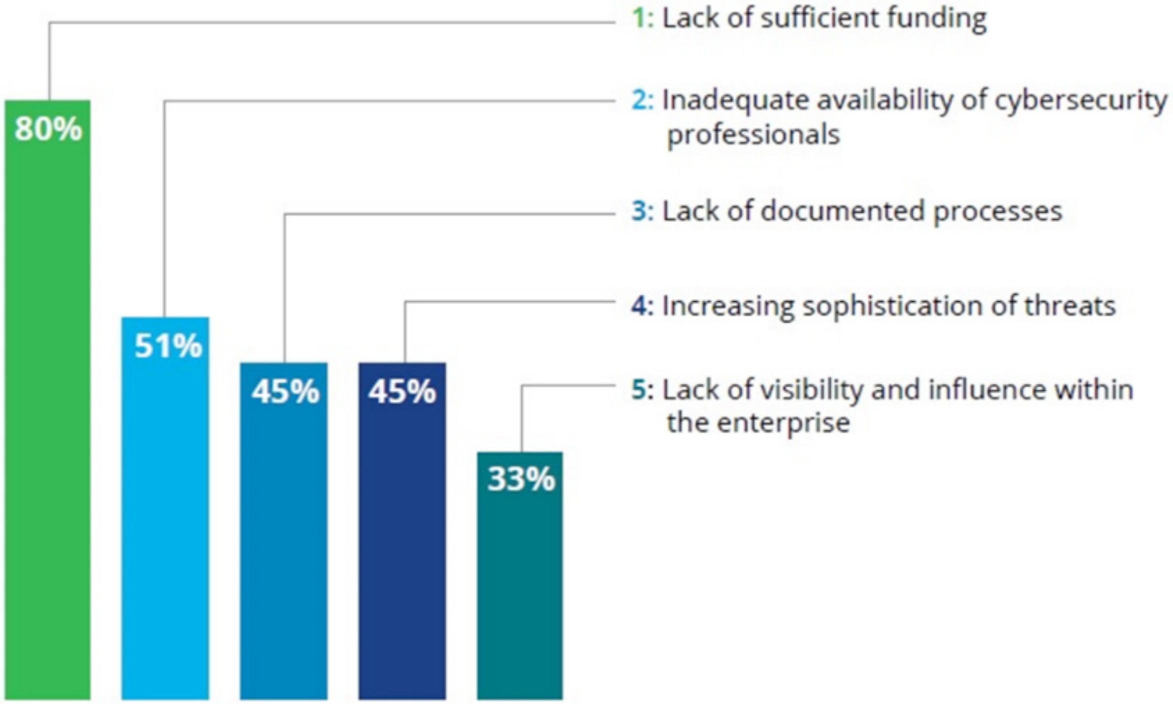
Lack of expertise, visibility and control, limited budgets, outdated/aging infrastructure, legacy systems and spending priorities are big factors causing state and local municipalities to fall victim to cyber-attacks.

According to a 2015 Ponemon Institute report:

- Cybersecurity practices are not clearly defined, according to 71 percent of state and local respondents.
- 50% of state and local governments experienced 6 to 25 breaches in the prior 24 months, and 12% experienced more than 25 breaches.
- Most state cyber budgets are between 0-2% of their overall IT budget, compared with an average of more than 10% in large companies.



Similarly, a 2016 NASCIO and Deloitte study indicated that 80% percent of state CIOs surveyed cited lack of sufficient funding as their number one challenge in cyber security, followed by inadequate availability of cyber security professionals.



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Beyond IT infrastructure, government entities are attractive targets for the wealth of data they control. Government data centers are a goldmine of high-value data like social security numbers, driver's license numbers and healthcare records.

A Cybersecurity Strategy is Your Best Defense

To combat the evolving cyber-threats facing government entities today, they must ensure they have an integrated approach to cybersecurity, tailored to address the broad scope of security needs that their constituency may face.

Here are a few cybersecurity strategy planning basics.

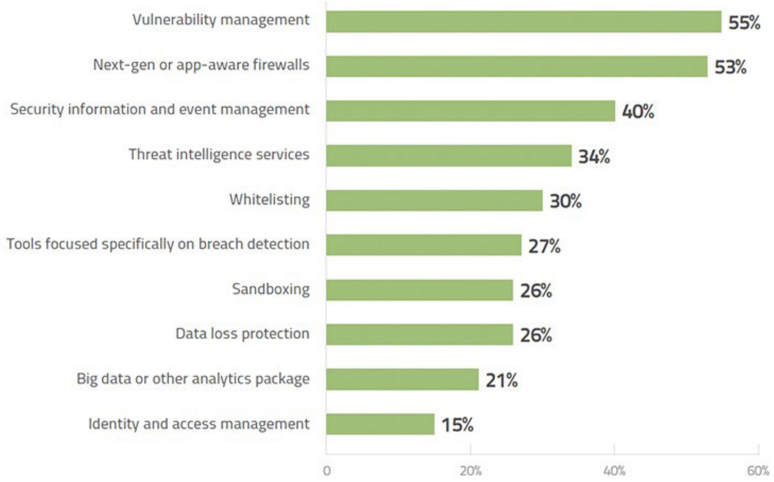
1. **Foster a Security Culture**
   According to TechTarget, sometimes the biggest security threat can come from within. Without the right environment, mindset and personnel, an organization's IT security is put at risk. Ensure that you promote a culture of security at your organization and educate your employees on security best practices.

2. **Perform a Security Assessment**
   Start with an extensive security assessment that will provide an accurate understanding of your organization's infrastructure to help you identify potential security risks and promote compliance with security best practices. The assessment should provide:

   a. An in-depth inspection of your entire IT infrastructure, looking for security weaknesses at your external Internet perimeter, as well as your internal user perimeter
   b. A review of your current security architectures and assessment of them against your policies, compliance needs and core security practices
   c. A review of your device configurations against best practices, your policies and compliance guidelines

3. **Establish Key Initiatives and Security Controls**
   Now that you have identified the risks, you must now select the most appropriate steps (or controls) to reduce these risks and further protect your critical data.

4. **Monitor and Test**
   It's impossible to prevent every attacker from gaining access to your critical data, but with the proper advanced threat detection and response tools in place, you can bolster your defenses.



Multiple Technologies Used in Advanced Threat Defense

Which of the following technologies have you deployed with defense against advanced threats as a key objective?

SOURCE: TECHTARGET, MAY 2015; BASED OFF RESPONSES FROM 380 IT AND BUSINESS PROFESSIONALS. RESPONDENTS COULD CHOOSE ALL THAT APPLY.

Your Trusted Cybersecurity Partner for State & Local Governments

State and local governments face a challenging new reality when implementing today's emerging technologies — a looming threat to constituent data security. Technologies such as mobility and the cloud are creating new — almost daily — opportunities for advanced, targeted attacks. It makes today's prevention strategies nearly inadequate for tomorrow.

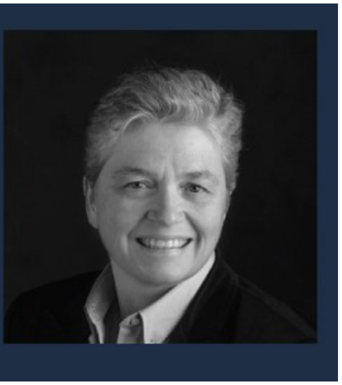
At OneNeck, we recognize threats can enter the network in a variety of ways. We understand that having comprehensive protection requires a multi-tiered and pervasive approach to keep threats out as well as detect and isolate any breaches quickly. We can assess your infrastructure for its strengths and weaknesses, then recommend and implement a solution that will keep your critical data safe.

Our solutions include:

- **Network Security.** End-to-end solutions from design architecture and deployment to configuration review related to all aspects of network security including firewalling, intrusion prevention sensors, VPNs, and traffic encryption/decryption.
- **Secure Application Delivery.** Protect your applications from external and internal threats with traffic managers and web application firewalls that offer SSL/TLS visibility & control, deep packet inspection, federated identity, and DDoS protection.
- **Web and email security.** The top two attack vectors for malware continues to be email and web browsing. You need a solution that uses advanced tactics to block malicious websites and emails whether on the corporate network or off.
- **Public/Private Cloud Security.** Protect your resources from incurring outages and your data from exfiltration through proper design, system segmentation, and access control. Identify shadow IT and public cloud risks by employing a cloud access security broker (CASB) solution.
- **Identity and Secure Access.** Provide authorized and secure access to your network with identity and secure access solutions.
- **Endpoint Security.** Running anti-virus with an encrypted HD isn't enough these days, you need a next-gen solution to prevent endpoints from being breached and remediating them if they are.
- **Secure Enterprise Mobility.** Enforce mobility policies, regulate behaviors, contain costs and manage risks across multiple device platforms with an MDM solution to address BYOD risks.
- **Security Monitoring and Threat Hunting.** You need to when a security threat is in progress so you can respond in time to protect against it. And since no security solution is 100% effective, you need a comprehensive SIEM solution in place to reduce you time to detection and breach remediation.
- **Security Assessments.** Security assessments using best practice or other industry standards like HIPAA or PCI are essential to identifying security and compliance risks and keeping your security program on track.

Looking for more than just cybersecurity? OneNeck provides an end-to-end, technology-independent approach that includes a complete suite of hybrid IT offerings across infrastructure, applications and managed services. This approach enables governments to realize benefits, not only internally but externally as well, leading to happier, more productive citizens.

Q&A with OneNeck Security Executive



Katie McCullough
VP Information Security & Business Applications

Q. Many experts maintain that the total cost of ransomware in 2016 was over a billion dollars – that's a staggering number. With the rate of sophisticated security attacks increasing at an alarming rate, how can an organization protect themselves from data leaks and/or malicious security attacks?

A. Focus on the basics. Make sure servers and workstations are properly patched, as known vulnerabilities that are years old continue to be a threat to companies (2016 Data Breach Investigations Report from Verizon). Constantly communicate and educate with your user base regarding the risks of malware and other fraud. And finally, be prepared with a plan, backups and other contacts for when something bad happens.

Q. Why are identity, credential and access management so critical in combatting today's security threats?

A. Credentials can be one of the weakest links to an environment. According to the Verizon Report, 63% of confirmed data breaches involved weak, default or stolen passwords.

So, start with the base philosophy of two fundamental principles: Least Access and Least Privilege.

- Least Access: Users shall be granted access only to those information assets necessary to perform their duties.
- Least Privilege: Users shall not be permitted any more than the least privileges necessary for processing the information assets to which they have been granted access.

Use and enforce good password practices (SANS Password Protection Policy). And invest in multi-factor authentication for your access into your core environment and critical systems.

Q. With the vast majority of enterprise businesses leveraging the cloud, it's no surprise that securing the critical data that's moving to the cloud is top of mind. What security considerations should an organization keep top of mind when evaluating a cloud provider?

A. Get to know the vendor and their operations. Talk to the cloud service provider's head of security, and understand their approach – what keeps them up at night. Do your due diligence get updated copies of compliance reports that the vendor provides. And finally, start small and invest in penetration testing and vulnerability scans of your environment.

Q. By enabling the convenience of "anywhere, anytime," we've seen an emergence of Shadow IT, where LOBs are bypassing IT in order to get things done. What recommendations would you give today's frustrated IT teams struggling to retain control and keep the infrastructure secure, all while dealing with rouge cloud services?

A. Security is all about risk management, and we have to be here to support the business in the tools and timing they need to get things done. The most important aspect is communication so you can at least do an assessment on what is being used by the business, how is it being accessed and who is handling the account management, what data is involved both transit and at rest, and what security do the cloud services have in place. Get it documented, and have the business sign off.

Q. As a provider of cloud, colocation and various advanced IT services, OneNeck has to keep security front and center to ensure we're not putting our customers at risk. In your role as OneNeck's VP of Information Security and Business Applications, what are you and your team doing to ensure the security of OneNeck's customer data?

A. Most important, staying involved with our customers and our operations to know what challenges they are dealing with and keeping them informed of risks to their business. We stay involved in the industry and with our vendors, to be aware of threats, how to prevent them or at least quickly detect and address any issues. And of course, leveraging the experience throughout the family of TDS companies to constantly evaluate and improve our security practices.

(855) ONE-NECK

www.OneNeck.com

OneNeck®
IT SOLUTIONS
a TDS® Company