Cisco 2018

Annual Cybersecurity Report

Impacts on Government

Table of Contents

Weaponizing technology to damage government services and infrastructure

Democracy's adversaries and multiple state-sanctioned actors now have the expertise and tools necessary to take down government networks. Even worse, they have shown the capability to damage critical infrastructure and services, crippling entire regions in the process. But are government agencies in America, at the local, state and federal levels, resilient enough?

For years, Cisco has been warning about escalating cybercriminal activity targeting networks around the world. In this condensed version of our 2018 Annual Cybersecurity Report, we will focus on how these activities are impacting the public sector. We will present data and analysis from Cisco threat researchers and several of our technology partners about attacker behavior observed over the past 12 to 18 months that has specifically targeted government. During that time we observed three key trends that are emerging in an attempt to weaponize technology to damage government services and infrastructure. These are:

1. **Taking malware to unprecedented levels of sophistication and impact**

The advent of network-based ransomware cryptoworms is eliminating the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but obliteration of systems and data. Self-propagating malware is dangerous and has the potential to take down the Internet, according to Cisco threat researchers.

2. **Increasing evasion and weaponizing cloud and other technologies**

Actors are embracing encryption to evade detection and adopting techniques that rely on legitimate Internet services like Google, Dropbox, and GitHub. The practice makes malware traffic almost impossible to identify. Also, many attackers are now launching multiple campaigns from a single domain and reusing infrastructure resources, such as registrant email addresses, autonomous system numbers (ASNs), and nameservers to get the best return on their investments.

3. **Exploiting undefended gaps in security for IoT and cloud services**

Unpatched and unmonitored IoT devices and cloud environments are giving attackers opportunities to infiltrate networks. IoT botnets are growing and becoming automated for advanced distributed-denial-of-service (DDoS) attacks. And organizations susceptible to attack seem unmotivated to fix the problem in a timely manner. Worse yet, such groups probably have more vulnerable IoT devices than they realize.

All statistics shown in this report are from the combined survey results from government, utilities, transportation, public safety and education categories in the original survey, unless otherwise noted.

About the report

The ***Cisco 2018 Annual Cybersecurity Report: Impacts on Government*** begins by providing a condensed version of our annual cybersecurity report and then expands on issues pertinent to specific areas of operations within the public sector. We also look at the techniques and strategies that adversaries use to break into and disrupt government networks and their defenses as well as how they evade detection. Lastly, we provide a list of recommendations for public sector security personnel to consider for strengthening their network defenses.

To view our annual report that provides a global perspective, please visit: Cisco 2018 Annual Cybersecurity Report.

Part I: The attack landscape

Adversaries are taking malware to unprecedented levels of sophistication and impact. The growing number and variety of malware types and families perpetuates chaos in the attack landscape by undermining government efforts to gain and hold ground on threats.

Evolving malware

One of the most important developments in the attack landscape against public sector resources in 2017 was the evolution of ransomware. The advent of network-based ransomware worms eliminates the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but the destruction of a government's systems and data, especially related to public safety and utilities. We expect this activity to increase.

Government agencies should be prepared to face new, self-propagating, network-based threats in 2018.

Ransomware continues to adapt

In May 2017, WannaCry, a ransomware cryptoworm, emerged and spread rapidly across the Internet. To propagate, it took advantage of a Microsoft Windows security vulnerability called EternalBlue. The malware struck government in its most critical areas: public safety and utilities. Agencies around the world, from Britain to Australia and even the United States, were successfully targeted. Even local government agencies, like the police and fire departments of Murfreesboro, Tennessee were impacted and data lost.

WannaCry earned more than US$143,000 through bitcoin payments at the point the wallets were cashed out. Cisco threat researchers estimate that roughly 312 ransom payments were made. Unfortunately, WannaCry did not track encrypted damage to and the payments made by affected users. So the number of users who received decryption keys after making a payment is unknown.

Due to the very low performance of WannaCry as ransomware, the U.S. government and many security researchers believe the ransom component is merely a smokescreen to conceal WannaCry's true purpose: wiping data.

Malware is increasingly clever

Nyetya (also known as NotPetya) arrived in June 2017. This wiper malware masqueraded as ransomware and also used the remote code execution vulnerability nicknamed "EternalBlue," as well as the remote code execution vulnerability "EternalRomance." Nyetya was deployed through software update systems for a tax software package installed on more than 1 million computers. In the Ukraine, it struck transportation and utilities critical to the nation's daily operations. This included a nuclear energy related facility and the nation's airports. Ukraine cyber police confirmed that it affected more than 2000 Ukrainian companies and government agencies.

One reason Nyetya was successful at infecting so many machines so quickly is that users did not see an automated software update as a security risk, or in some cases even realize that they were receiving the malicious updates. For today's self-propagating malware, an active and unpatched workstation is all that is needed to launch a network-based ransomware campaign.

WannaCry and Nyetya could have been prevented, or their impact muted, if more organizations had applied basic security best practices such as patching vulnerabilities, establishing appropriate processes and policies for incident response, and employing network segmentation.

For more tips on meeting the threat of automated network-based ransomware worms, read ***Back to Basics: Worm Defense in the Ransomware Age*** on the Cisco Talos blog.

Encrypted malicious web traffic

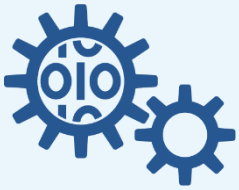
The expanding volume of encrypted web traffic, both legitimate and malicious, creates even more challenges and confusion for the public sector as it tries to identify and monitor potential threats. Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool to conceal command-and-control (C2) activity, affording them more time to operate and inflict damage. Cisco threat researchers expect to see adversaries increase their use of encryption in 2018. To keep pace, government will need to incorporate more automation and advanced tools like machine learning and artificial intelligence to complement threat prevention, detection, and remediation.

There's a hole in government security, and it's attracting more attention.

The need to adopt machine learning and artificial intelligence

Cisco threat researchers report that 50 percent of global web traffic was encrypted as of October 2017. As that volume grows, adversaries appear to be widening their embrace of encryption as a tool for concealing their activity. Cisco threat researchers observed a more than threefold increase in encrypted network communication used by inspected malware samples over a 12-month period. Our analysis of more than 400,000 malicious binaries found that about 70 percent had used at least some encryption as of October 2017.

To overcome the lack of visibility that encryption creates, and reduce adversaries' time to operate, we see more organizations exploring the use of machine learning and artificial intelligence (AI). These advanced behavioral analytics capabilities can enhance network security defenses and, over time, "learn" how to automatically detect unusual patterns in web traffic that might indicate malicious activity.



Machine learning is useful for automatically detecting "known-known" threats, the types of infections that have been seen before. But its real value, especially in monitoring encrypted web traffic, stems from its ability to detect "known-unknown" threats (previously unseen variations of known threats, malware subfamilies, or related new threats) and "unknown-unknown" (net-new malware) threats.

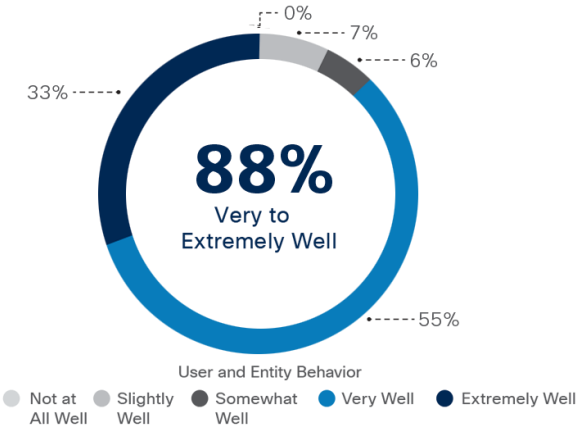
These technologies can learn to identify unusual patterns in large volumes of encrypted web traffic and automatically alert government security teams to investigate further. That is especially important, given that many government agencies traditionally lack sufficient personnel to address security issues. Automation and intelligent tools like machine learning and artificial intelligence can help government IT teams overcome skills and resource gaps, making them more effective at identifying and responding to both known and emerging threats.

The value of behavioral analytics becoming clear

Fortunately, as revealed in the Cisco 2018 Security Capabilities Benchmark Study, government agencies are increasingly on board with the value of behavioral analytics, with 55% feeling it can serve them very well and another 33% feel it can serve them extremely well. This data reveals that a full 88% of government security professionals feel they have a good understanding of the value that behavioral analytics can bring to their cybersecurity initiatives. This is a good sign, and indicative that past efforts to educate the public sector on emerging technologies is bearing fruit.

Most government security professionals see value in behavioral analytics tools

Source: Cisco 2018 Security Capabilities Benchmark Study



A key reason for this increase in awareness has likely been the Continuous Diagnostics and Mitigation (CDM) program created by the Department of Homeland Security (DHS). It includes direction on behavioral analytics pertaining to ongoing identification of cybersecurity risk, prioritization based on potential impacts, and mitigation. For more information visit: DHS CDM program.

Email threats

No matter how much the threat landscape changes, malicious email and spam remain vital tools for adversaries to distribute malware throughout the public sector, because they take threats straight to the endpoint. By applying the right mix of social engineering techniques, such as phishing and malicious links and attachments, adversaries can sit back and wait for unsuspecting users, who may be connecting through a government network, to activate the exploits.

Using archive files to hide future attacks is still a key danger.

Archive files still heavily used to plan attacks

Cisco threat researchers analyzed email telemetry from January through September 2017 to identify the types of malicious file extensions in email documents that common malware families employed most often. The analysis yielded a top 10 list that shows the most prevalent group of malicious file extensions (38 percent) was Microsoft Office formats such as Word, PowerPoint, and Excel.

Archive files, such as .zip and .jar, accounted for about 37 percent of all the malicious file extensions observed in our study. That adversaries heavily employ archive files is not surprising, as they have long been favored hiding places for malware.

Adversaries also use obscure file types, such as .7z and .rar, to evade detection. Malicious PDF file extensions rounded out the top three in our analysis, accounting for nearly fourteen percent of malicious file extensions observed.

Our analysis of malicious file extension types shows that even in today's sophisticated and complex threat environment, email remains a vital channel for malware distribution. For government agencies, baseline defense strategies should include:

- Implementing powerful and comprehensive email security defenses.
- Continually educating users about the threat of malicious attachments and links in phishing emails and spam.

Old threat still fresh as tactics to execute evolve

Social engineering is also a critical launching pad for email attacks. Phishing and spear phishing are well-worn tactics for stealing users' credentials and other sensitive information, and that's because they are very effective. From January to August 2017 we found that threat actors were employing 326 unique TLDs (top-level domains) for these activities, including .com, .org, .top plus some country-specific TLDs.

Government agencies should remain vigilant in monitoring this "old" threat. Some of the common tactics and tools adversaries use to execute phishing campaigns include:

- Domain squatting: Domains named to look like valid domains (example: cisc0[dot]com).
- Domain shadowing: Subdomains added under a valid domain without the owner's knowledge (example: badstuff[dot]cisco[dot]com).
- Maliciously registered domains: A domain created to serve malicious purposes (example: viqpbe[dot]top).
- URL shorteners: A malicious URL disguised with a URL shortener (example: bitly[dot]com/random-string).
- Subdomain services: A site created under a subdomain server (example: mybadpage[dot]000webhost[dot]com).

Fortunately, as of Jan. 15, 2018 all federal agency domains are required to have Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (DMARC) records in place. You can learn more about this DHS order at Binding Operational Directive 18-01.

Sandbox evasion tactics

Adversaries are becoming adept at developing threats that can evade increasingly sophisticated sandboxing environments. When Cisco threat researchers analyzed malicious email attachments that were equipped with various sandbox evasion techniques, they discovered that the number of malicious samples using a particular sandbox evasion technique showed sharp peaks, and then quickly dropped. This is yet another example of how attackers are swift to ramp up the volume of attempts to break through defenses once they find an effective technique.

Malware authors playing clever tricks in government sandboxes?

Using loopholes as triggers to unleash havoc

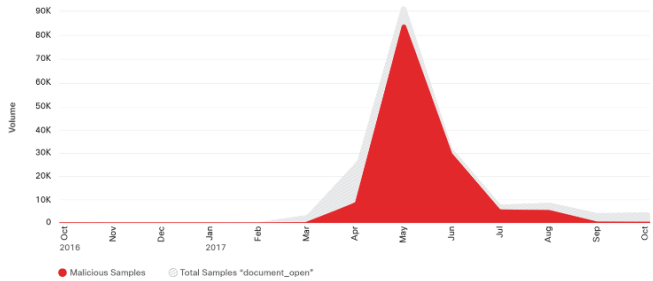
In September 2017, Cisco threat researchers noted high volumes of samples where a malicious payload is triggered using the "document close" event. The technique works because, in many cases, documents are not closed after the document has been opened and analyzed in a "sandbox."

> Sandboxing is when a program is moved to a separate, isolated area while it runs, so that if errors or security issues occur, they will not spread to other areas on the computer

Because the sandbox doesn't explicitly close the document, the attachments are deemed safe by the sandbox, and will be delivered to the intended recipients. When a recipient opens the document attachment, and later closes the document, the malicious payload is delivered. Sandboxes that don't properly detect actions on document close can be evaded using this technique.

Attackers use PDFs with embedded Microsoft Word documents to evade sandboxing

Source: Cisco Security Research



The use of the "document close" event is a clever option for attackers. It takes advantage of macro functionality built into Microsoft Office, and a user's tendency to open attachments that they believe are relevant to them. Once users realize the attachment is not relevant to them, they close the document, triggering the macros in which the malware is hidden. This method of delivering malicious payloads is widespread in the public sector since governments, especially at the state and local level, generally use Microsoft products and often move working documents across devices for review or action.

Some attackers evade sandboxing by disguising the type of document in which the malicious payload exists. We noted a significant attack in May 2017 that was built around malicious Word documents embedded within PDF documents. The documents might bypass sandboxes that simply detect and open the PDF, instead of also opening and analyzing the embedded Word document. The PDF document typically contained an enticement for the user to click and open the Word document, which would trigger the malicious behavior. Sandboxes that don't open and analyze documents embedded within PDFs can be bypassed using this technique.

Content-aware features key to lowering risks

After viewing the spike in malicious samples involving these PDFs, our threat researchers refined the sandbox environment to detect whether PDFs contained actions or enticements to open embedded Word documents.

The spikes in malicious samples using different sandbox evasion techniques point to malicious actors' desire to follow a process that seems to work for them—or for other attackers. Also, if adversaries go to the trouble of creating malware and associated infrastructure, they want a return on their investments. If they determine that malware can slip through sandbox testing, they will, in turn, increase the number of attack attempts and affected users.

Cisco researchers recommend government agencies use sandboxing that includes "content-aware" features to help ensure malware that uses the tactics described above does not evade sandbox analysis. For example, sandboxing technology should show awareness of the metadata features of the samples it is analyzing—such as determining whether the sample includes an action upon closing of the document.

Abuse of cloud services and other legitimate resources

As applications, data, and identities move to the cloud, often under mandate, the public sector must manage the risk involved with losing control of the traditional network perimeter. Attackers are taking advantage of the fact that security teams are having difficulty defending, evolving, and expanding government cloud and IoT environments. One reason is often the lack of clarity around who exactly is responsible for protecting those environments. To meet this challenge, public sector agencies may need to apply a combination of best practices, advanced security technologies like machine learning, and even some experimental methodologies, depending on the cloud services they use and how threats in this space evolve.

Malicious use of legitimate resources for backdoor command and control.

Threats hiding within legitimate cloud-based services

When threat actors use legitimate services for command and control (C2), malware network traffic becomes nearly impossible for government agencies to identify because it mimics the behavior of their legitimate network traffic. Adversaries have a lot of Internet "noise" to use as cover because many in the public sector may rely on cloud-based services like Google Docs and Dropbox to do their work, regardless of whether these services are offered or systemically endorsed by their agencies.

Using legitimate cloud-based services for C2 appeals to malicious actors because it's easy to:

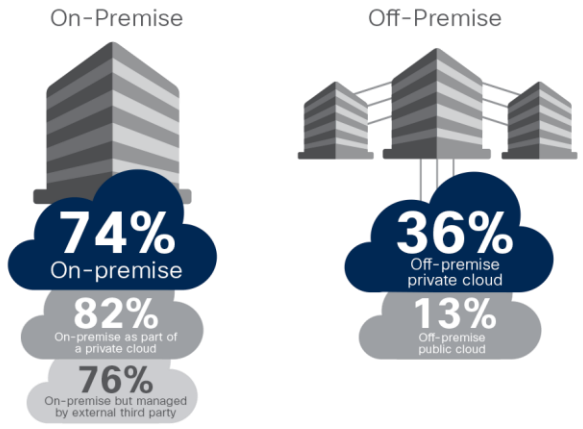
- Register new accounts on these services.
- Set up a web page on the publicly accessible Internet.
- Usurp encryption for C2 protocols (Instead of setting up C2 servers with encryption or building encryption into malware, attackers can simply adopt the SSL certificate of a legitimate service).
- Adapt and transform resources on the fly (Attackers can reuse implants across attacks without reusing DNS or IP addresses, for instance).
- Reduce the likelihood of "burning" infrastructure (Adversaries that use legitimate services for C2 don't need to hard-code malware with IP addresses or domains. When their operation is complete, they can simply take down their legitimate services pages—and no one will ever know the IP addresses).
- Reduce overhead and improve their return on investment.

More governments moving to private clouds

The Cisco 2018 Security Capabilities Benchmark Study revealed a strong move to the cloud by government agencies, with a clear preference (74%) for on-premise cloud. Yet this preference is still split fairly evenly between operating their own private cloud (82%) or using a third party to manage it for them (76%).

More public sector agencies are using private clouds

Source: Cisco 2018 Security Capabilities Benchmark Study



For government security workers, an adversary's use of legitimate services for C2 presents some significant challenges:

- Legitimate services are difficult to block, such as some Google apps or social promotion platforms that government employees may use on a daily basis.
- Legitimate services are often encrypted and innately difficult to inspect, plus SSL decrypting is expensive and not always possible at a large scale. So malware hides its communication inside of encrypted traffic, making it difficult, if not impossible, for security teams to identify malicious traffic.
- Use of legitimate services subverts domain and certificate intelligence, and complicates attribution. Adversaries don't need to register domains because the legitimate service account is considered the initial C2 address.

Using intelligent, first-line-of-defense cloud security tools to identify and analyze potentially malicious domains and

Eighty-two percent of public sector agencies host at least 50% of infrastructure in the cloud

Source: Cisco 2018 Security Capabilities Benchmark Study

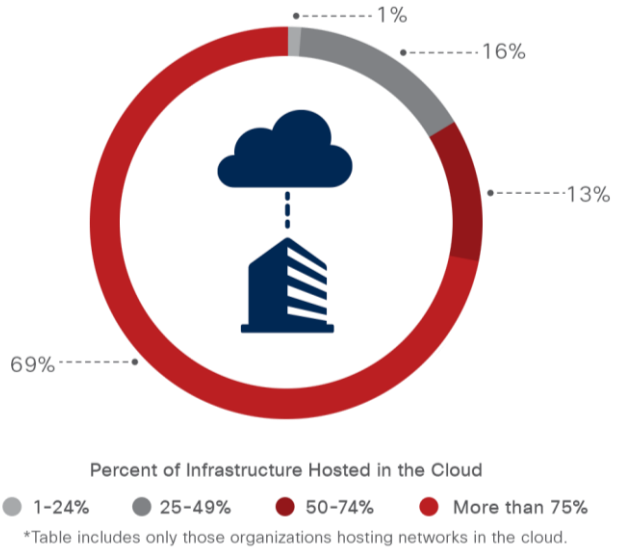


*Table includes only those organizations hosting networks in the cloud.

subdomains can also help government security teams follow the trail of an attacker to find actual IP addresses, ASNs, and registrants of malicious domains. The answers can help defenders refine their network security policies and block attacks, plus prevent personnel and other users from connecting to malicious destinations on the Internet while they're on the agency's network.

Insider threats and the cloud

Unfortunately, the cloud can be an avenue for insider threats to propagate. To further examine the impact of user activity on security, Cisco threat researchers recently examined data exfiltration trends. They employed a machine-learning algorithm to profile 150,000 users in 34 countries, all using cloud service providers, from January to June 2017. The algorithm accounted for not only the volume of documents being downloaded, but also variables such as the time of day of downloads, IP addresses, and locations.

After profiling users for six months, our researchers spent 1.5 months studying abnormalities, flagging 0.5 percent of users for suspicious downloads. That's a small amount, but these users downloaded, in total, more than 3.9 million documents from cloud-based systems, or an average of 5200 documents per user during the 1.5-month period. Of the suspicious downloads, sixty-two percent occurred outside of normal work hours; fourty percent on weekends.

Cisco researchers also conducted a text-mining analysis on the titles of the 3.9 million suspiciously downloaded documents. One of the most popular keywords in the documents' titles was "data." The keywords most commonly appearing with the word "data" were "employee" and "customer." Of the types of documents downloaded, thirty-four percent were PDFs and thirty-one percent were Office documents.

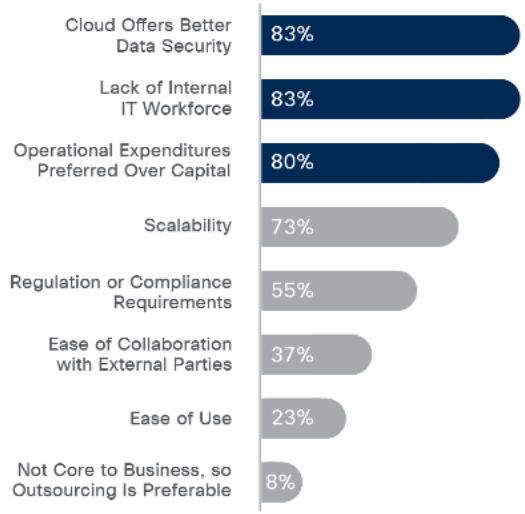
In our analysis, twenty-three percent of the users we studied were flagged more than three times for suspicious downloads, usually starting with small numbers of documents. The volume slowly increased each time, and eventually, these users showed sudden and significant spikes in downloads.

Machine learning key to greater visibility into cloud

Our benchmark study also found that eighty-three percent of public sector agencies select cloud because they feel it offers better data security. The good news is that by applying machine-learning algorithms to their cloud environments, government agencies can get a more nuanced view of cloud user activity beyond just the number of downloads.

Eighty-three percent of public sector agencies select cloud because it offers better data security

Source: Cisco 2018 Security Capabilities Benchmark Study



For governments, machine-learning algorithms hold the promise of providing greater visibility into the cloud and user behavior. If an agency's IT team can start predicting user behavior in terms of downloads, they can save the time it might take to investigate legitimate behavior. They can also step in to stop a potential attack or data-exfiltration incident before it happens. Respondents also said that, as more infrastructure is moved to the cloud, they may look to invest in cloud access security brokers (CASBs) to add extra security to cloud environments.

IoT and DDoS attacks

The IoT is still evolving, but adversaries are already exploiting security weaknesses in IoT devices, such as security cameras and tablets, to gain access to public sector networks. This includes control systems that support critical infrastructure for power, water, and communications. IoT botnets are also growing in both size and power, and are increasingly capable of unleashing powerful attacks that could severely disrupt the Internet, cutting access by government personnel during times of emergencies. Attackers' shift toward greater exploitation of the application layer indicates that this is their aim. But many government security professionals aren't aware of, or dismiss, the threat that IoT botnets pose. Organizations keep adding IoT devices to their IT environments with little or no thought about security, or worse, take no time to assess how many IoT devices are touching their networks. In these ways, they're making it easy for adversaries to take command of key government assets.

Few governments see IoT botnets as an imminent threat, but they should.

Could IoT botnets be a major threat to infrastructure?

As the IoT expands and evolves, so too are IoT botnets. And as these botnets grow and mature, attackers are using them to launch distributed denial of service (DDoS) attacks of increasing scope and intensity against government agencies ranging from public safety, transportation, utilities and even national defense (watch: Anatomy of an IoT Attack).

Research by Cisco partner Radware recently found that only 13 percent of all organizations surveyed believe that IoT botnets will be a major threat in 2018. But IoT botnets could rapidly grow as a threat as the public sector increases use of low-cost IoT devices, often with little or no regard to their security. Most government IoT devices operate 24/7, such as tablets in a patrol car or EMS vehicle, or chemical sensors near an industrial plant, and could be quickly exploited.

Application DDoS overtakes network DDoS

Application layer attacks are on the rise while network layer attacks are declining. Radware researchers suspect this shift can be attributed to growth in IoT botnets. The trend is concerning because the application layer is so diverse, and has so many devices within it, which means attacks targeting this layer could potentially shut down much of the Internet.

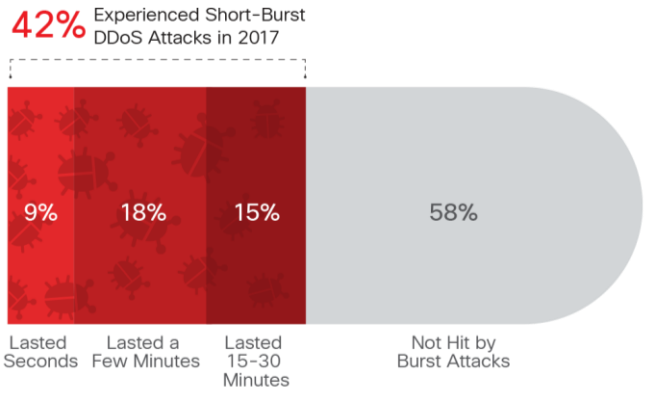
More attackers are turning to the application layer because there is little left to exploit in the network layer. IoT botnets are also less resource-intensive than PC botnets to build. That means adversaries can invest more resources in developing advanced code and malware.

"Burst attacks" on the rise

One of the most significant DDoS attack trends observed in 2017 was an increase in short-burst attacks, which are becoming more complex, frequent, and persistent. Forty-two percent of organizations in Radware's investigation experienced this type of DDoS attack in 2017. In most of the attacks, the recurring bursts lasted only a few minutes.

Experience with DDoS attacks in recurring bursts

Source: Radware



Growth in reflection amplification attacks

Reflection amplification DDoS attacks are also increasing. They use a potentially legitimate third-party component to send attack traffic to a target, concealing the attacker's identity. Attackers send packets to the reflector servers with a source IP address set to the target user's IP. That makes it possible to indirectly overwhelm the target with response packets and exhaust the target's utilization of resources.

Defenders must remediate "leak paths"

A "leak path," as defined by Cisco partner Lumeta, is a policy or segmentation violation or unauthorized or misconfigured connection created to the Internet on an enterprise network, including from the cloud, that allows traffic to be forwarded to a location on the Internet, such as a malicious website.

These unexpected connections can also occur internally between two different network segments that should not be communicating with each other. For example, in critical

infrastructure environments like a power plant, an unexpected leak path between controls located at the source of power generation and the business IT systems could indicate malicious activity. Leak paths can also stem from improperly configured routers and switches.

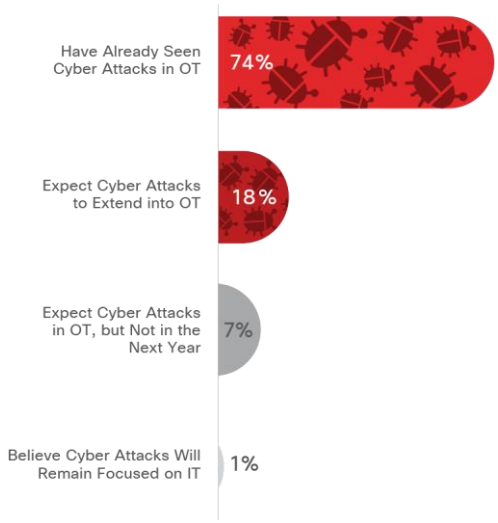
Detection of newly created leak paths in real-time is critical since they are immediate indicators of compromise and are associated with most advanced attacks, including ransomware.

Industrial control systems vulnerabilities place critical infrastructure at risk

Industrial control systems (ICS) are at the heart of all operations and process control systems for today's infrastructure (water, waste, power, communications). ICS connect to other electronic systems that are part of the control process, creating a highly connected ecosystem of vulnerable devices that a wide range of attackers is eager to compromise.

Seventy-four percent of public sector agencies have experienced cyber attacks on OT infrastructure

Source: Cisco 2018 Security Capabilities Benchmark Study



Threat actors, including nation-states and terrorist organizations, who want to target ICS to cripple critical infrastructure are actively engaged in research and creating backdoor pivot points to facilitate future attacks, according to TrapX Security, a Cisco partner that develops deception-based cybersecurity defenses. They recently conducted investigations into several cyber attacks that targeted ICS.

One was a large international water treatment and waste processing company. Attackers used the company's demilitarized zone (DMZ) server as a pivot point to compromise the internal network. The security operations team received alerts from deception security technology embedded in the network DMZ. This physical or logical subnetwork bridges internal networks from untrusted networks, such as the Internet, protecting other internal infrastructure. The investigation found that:

- The DMZ server was breached due to a misconfiguration that allowed RDP connections.
- The server was breached and controlled from several IPs, which were connected to political hacktivists.
- The attackers were able to launch multiple major attacks against several of the organization's other plants, from the compromised internal network.

The second target focused on energy. A power plant's critical assets include a very large ICS infrastructure and the necessary supervisory control and data acquisition (SCADA) components that manage and run their processes. The plant is considered critical national infrastructure and subject to scrutiny and oversight by the responsible national security agency. It is therefore considered a high-security installation.

The Chief Information and Security Officer (CISO) involved decided to implement deception technology to protect the plant's standard IT resources from ransomware attacks and found that:

- A device in the process control network was attempting to map and understand the exact nature of each PLM controller within the network.
- A vendor performing maintenance failed to close a connection when finished, leaving it vulnerable.

Threat researchers with TrapX recommend that organizations take the following actions to reduce risk:

- Review vendors and systems, and see that all patches and updates are applied promptly.
- Reduce the use of USB memory sticks and DVD drives.
- Isolate ICS systems from IT networks and don't allow any direct connections between the two.
- Implement policies that severely limit the use of the ICS networks for anything other than essential operations.
- Research and eliminate all embedded passwords or default passwords in your production network and wherever possible, implement two-factor authentication.
- Review your plans for disaster recovery following a major cyber attack.

For additional case studies and to better understand the threats governments are facing with IoT and DDoS attacks, see the TrapX Security research paper, Anatomy of an Attack: Industrial Control Systems Under Siege.

Vulnerabilities

There was a time when patching known vulnerabilities within 30 days was considered best practice. Now, waiting that long to remediate could increase a public sector agency's risk of being targeted for attack because threat actors are moving faster to release and use active exploits of vulnerabilities. Government should avoid neglecting small but significant security gaps that could benefit adversaries, especially during the reconnaissance phase of attacks when they are searching for pathways into systems.

The IoT is an increasing focus for attacks on government.

IoT and library vulnerabilities loomed larger in 2017

We know that attackers are evolving and adapting their techniques at a faster pace than defenders. They are also weaponizing and field testing their exploits, evasion strategies, and skills so they can launch attacks of increasing magnitude.

Between October 1, 2016, and September 30, 2017, Cisco threat researchers discovered 224 new vulnerabilities in non-Cisco products, of which forty vulnerabilities were related to third-party software libraries included in these products, and seventy-four were related to IoT devices. Public sector defenders should assume that third-party software libraries can be targets for attackers and:

- Check frequently for patches.
- Review security practices of third-party vendors.
- Ensure auto-update is running securely.

Active exploits fuel race to remediate

Qualys, Inc., a Cisco partner and provider of cloud-based security and compliance solutions, took a retrospective look at patch management behavior across several industries before and after the WannaCry campaign of May 2017.

> Qualys' research indicates it takes a major event to motivate many governments to patch critical vulnerabilities. Even knowledge of an active exploit is not enough to accelerate remediation, noting a patch for WannaCry was available.

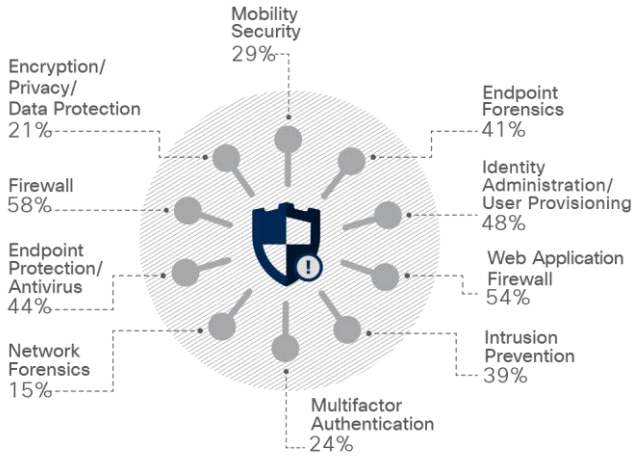
This revealed that unknown, unmanaged, rogue, and shadow IT endpoints were left unpatched. As a result, attackers were able to leverage these blind spots.

Patching is slower, or non-existent, for IoT devices

Qualys also examined patching trends for IoT devices, finding that eighty-three percent in their sample had critical vulnerabilities. This might have been due to the devices not being updatable or requiring direct support from the vendor. Also, it is not always clear who inside government is responsible for maintenance of IoT devices. And as in most cases, lack of personnel has an impact.

Key capabilities public sector defenders would add, if staffing levels improved

Source: Cisco 2018 Security Capabilities Benchmark Study



Most common vulnerabilities are low severity, high risk

Low-severity vulnerabilities are often left unremediated for years because agencies don't know they exist or don't consider them significant risks, according to security experts with SAINT Corporation, a security solutions company and Cisco partner. However, these small but significant security gaps could provide adversaries with pathways into systems.

Taking steps to reduce risk

A first step to addressing these issue is inventorying all IoT devices on the network. Agencies can then determine whether the devices are scannable and still supported by vendors, and which employees in the company own and use them. Government can also improve IoT security by treating all IoT devices like other computing devices and make sure they receive firmware updates and are patched regularly.

The defender landscape

We know that attackers are evolving and adapting their techniques at a faster pace than public sector defenders. They are also weaponizing and field testing their exploits, evasion strategies, and skills so they can launch attacks of increasing magnitude. When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover? That depends largely on the steps they're taking today to strengthen their security posture.

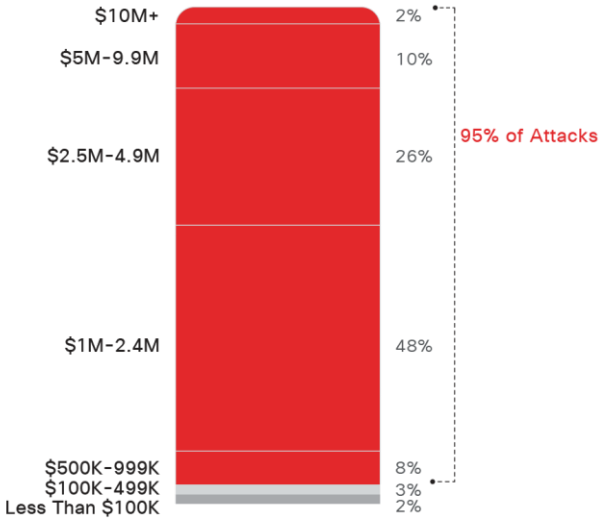
Understanding impacts and challenges.

The cost of attacks

The fear of breaches is founded in the financial cost of attacks, which is no longer a hypothetical number. Breaches cause real economic damage to public sector organizations, damage that can take months or years to resolve. According to study respondents, a startling ninety-five percent of all attacks against public sector entities resulted in financial damages of more than US$500,000, including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket costs.

Ninety-five percent of attacks result in damages of $500,000 or more

Source: Cisco 2018 Security Capabilities Benchmark Study



Challenges and obstacles

In their efforts to protect government, security teams face many roadblocks. Due to its nature, serving a broad continuum of citizen needs, government must defend several areas and functions, which adds to security challenges. Key challenges they report facing involve mobile devices, data in the public cloud, and user behavior.

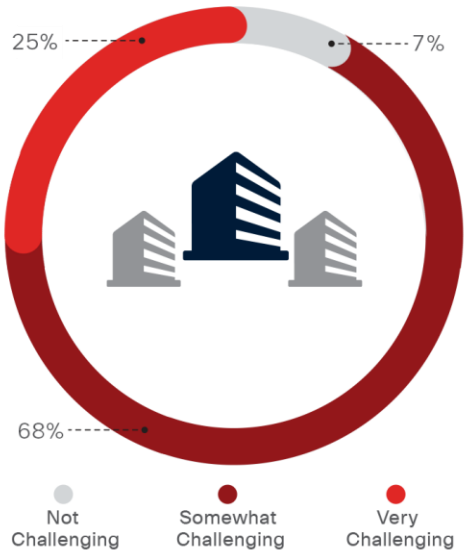
Lack of skilled talent tops the list of obstacles in all industries and across all regions. While the skilled talent gap is an ongoing challenge, organizations report that they're seeking out and hiring more resources for their security teams.

Complexity created by vendors in orchestration

Public sector defenders are implementing a complex mix of products from a cross-section of vendors: an arsenal of tools that may muddy rather than clarify the security landscape.

The challenge of orchestrating alerts in the public sector

Source: Cisco 2018 Security Capabilities Benchmark Study



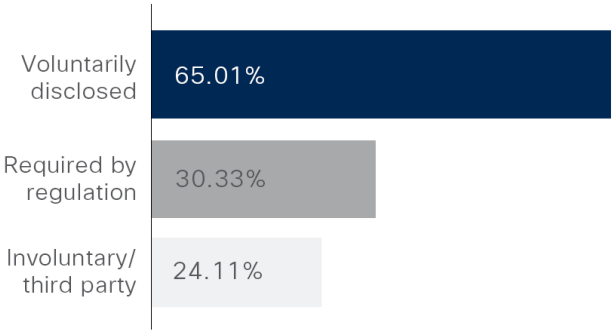
This complexity has many downstream impacts for orchestrating alerts, with data indicating that gaps continue to exist between alerts generated, those that have been investigated, and those that are eventually remediated. This process leaves many legitimate alerts unremediated. One reason appears to be the lack of headcount and trained personnel who can facilitate the demand to investigate all alerts.

Public scrutiny from breaches, higher risk of losses

Former Cisco CEO John Chambers said it best: "There are two types of organizations: those who have been hacked, and those who don't yet know they have been hacked." Even though public sector agencies are doing their best to meet future security challenges with adequate preparation, security professionals expect they'll fall victim to a breach that receives public scrutiny.

Sixty-five percent of public sector organizations voluntarily disclosed breaches

Source: Cisco 2018 Security Capabilities Benchmark Study



*Includes only public sector organizations that managed public scrutiny due to security breaches (government, transportation, utilities, defense, and education).

The potential damage in public trust and to citizens' private data because of a breach cannot be underestimated. In addition, the difficulty in managing public scrutiny of a breach, especially in regards to media relations and reassuring the public, can cause significant strain on limited resources during a time of already increased chaos. But it is best for parties involved for the public sector to be as transparent as possible during these events. Voluntary disclosure of a breach can be valuable in maintaining public trust. Our survey found, of those having to manage public scrutiny due to a breach, over sixty-five percent voluntarily disclosed the breach rather than others doing it for them.

Addressing people and policies, as well as technology

Faced with potential losses and adverse impact on systems, public sector organizations need to move beyond relying solely on technology for defense. That means examining other opportunities to improve security, such as applying policies or training users. This holistic approach to security can be centered on three key defensive capabilities: people, policies, and technology.

Some issues, such as weak passwords, cross over all three categories. Strengthening passwords can require improvements in people (user training), products (configuring servers for more complex passwords), and policies (setting stronger password requirements).

The public sector can increase its odds of successfully managing all three factors if it ensures that security is embedded into every layer of the organization and not bolted on here and there. They should also avoid relying solely on products or technical improvements to fix security. Because for products to work correctly, agencies need to understand and implement sensible support policies and processes first.

Investing in technology and training

Our research indicated that security professionals fully anticipate that the threats facing the public sector will remain complex and challenging. They expect bad actors to develop more sophisticated and damaging ways to breach networks. And they understand that the modern workplace creates conditions that favor the attackers as the mobility of employees and adoption of IoT devices provide fresh opportunities. Along with increased threats, many government security personnel expect they'll be under additional scrutiny from regulators, politicians, agency leaders, vendors, and especially citizens. Yet for those public sector organizations that have had to deal with public scrutiny after a breach, ninety-five percent felt it became the primary driver of improving their security posture.

To reduce the likelihood of risk and losses, public sector defenders must determine where to invest finite resources. When planning budgets, agencies must earmark sufficient funds to initiate viable security plans, prioritizing investments as more budget becomes available. And they should be ready to quickly seek additional funding avenues if new vulnerabilities are exposed, whether by an internal incident, a highly publicized public breach, or a routine third-party risk assessment.

Government should also begin allocating a portion of budgets toward tools that use artificial intelligence and machine learning. These funds may not always be additional expenditures but merely a shifting of resources since they may often help reduce costs elsewhere by improving defenses, reducing unseen costs for remediation, and automating workload to free personnel for other projects. Government agencies should also consider outsourcing services, such as network management, cloud, technical support, and training to stretch resources and strengthen defenses. In addition, agencies should plan to invest in tools that will provide safeguards for critical systems, such as critical infrastructure services (water, sewer, operations centers and even 911 services).

Part II: Impacts on Governance

As adversaries increasingly target the public sector, their goals become more varied. While financial rewards continue to be a top priority, more emphasis is being placed on the destruction of data and damaging key infrastructure. And there appears to be a clear attempt to disrupt governance and sow seeds of distrust and fear.

A challenge to freedom and quality of life

Over the last year, nation-states and other actors have worked tirelessly to elevate their attacks against governments in the United States. From the state and local level, to federal, and even education, adversaries have shown clear intent to damage our form of government. As a result, networks for operations, utilities, transportation, public safety, education and national defense must gain greater resilience if we are to preserve the processes which ensure our freedoms and quality of life.

Government agencies must secure data and infrastructure in a way that promotes resilience of governance and public services.

Three areas government must lead

Governments at all levels maintain a massive amount of data that is used to directly impact the services they provide citizens. Every day this data is used to maintain and improve the quality of life we enjoy. From reducing traffic jams and speeding response times to emergencies, or ensuring utilities stay online during severe weather, data has become a key player in the public sector. Securing the collection, aggregation, and storage of it can be difficult. But failure to do so can be detrimental.

Did you know? Cyber attacks were declared a national emergency by President Obama in 2015. This executive order was set to expire on April 1, 2018 but due to ongoing threats to government services and infrastructure, was extended for one year by President Trump, who stated *"significant malicious cyber-enabled activities continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."*

Many government networks may be connected to larger databases and networks, increasing the opportunity for spreading malicious attacks and cascading damage. In today's connected world, an attack against a lone agency at the state level could inadvertently spread malware to local or even federal networks, and vice-versa. This could result in permanent loss of data (personal, financial and health), key utilities being taken off-line for extended periods of time (energy, water, communications), and delay in emergency response (EMS, fire and rescue, law enforcement).

The increasing number of cyber attacks against the public sector could put significant amounts of private citizen data and our nation's infrastructure at direct risk. So it is critical that governments take the lead in:

- Securing agency and private citizen data.
- Keeping key infrastructure and assets secure.
- Staying ahead of emerging technologies used by adversaries.

The need for resilience in government

At the same time, the public sector must find ways to protect itself and citizens without limiting the very freedoms and quality of life they are charged with defending. To do otherwise would result in victory for our adversaries. This means the public sector must develop resilient data and infrastructure processes that allow government to survive during, and rebound quickly after, incidents.

Resilience should go beyond the public sector to include a partnership between government, industry, and citizens. This will require a transparency on government's part that is built

upon strong community engagement (learn more here). By doing so, government can develop the capabilities to survive, adapt, and grow in the face of the continual stresses and intense shocks that may result from cyber attacks, as well as everyday events.

Three trends government should be aware of

As the public sector increases its focus on securing data, protecting infrastructure, and staying ahead of adversaries, there are three important trends, both good and bad, shaping up for 2018:

- The overwhelming adoption of cybersecurity frameworks based on national standards and guidelines (such as NIST and CJIS).
- The appearance of self-propagating, network-based threats.
- The rise of cryptojacking.

Establishing a framework

Many organizations, such as the FBI and the National Institute of Standards and Technology (NIST), have used knowledge gained in cyber warfare to develop best practices and approaches that can be adapted or used as-is by other government entities. These include the NIST Cybersecurity Framework and the FBI's Criminal Justice Information Services (CJIS) Security Policy. Combined with a threat-centric approach to cybersecurity, they can help deter and reduce impacts from attacks.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a proven collaborative effort by both the private sector and public sector. It can provide the public sector with a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on organizations.

Emergence of self-propagating threats

The WannaCry attack of May 2017 was a next-generation ransomware, called a cryptoworm. It did not need help to spread because it was a self-propagating, network-based attack. How did it work? By exploiting a known but often overlooked vulnerability. Once one Windows user's operating system was infected and on a Windows network, WannaCry spread by itself, without human interaction, infecting and encrypting other unpatched devices. It proved very successful, infecting networks and devices around the world, including energy and transportation systems.

The method worked so well that we can expect other groups, especially hostile nation-states, to adopt its use and most likely escalate the damage it can inflict on government assets. But the appearance of cryptojacking may be the most significant of all.

Hidden codes taking toll

Cryptojacking involves an adversary discretely inserting code into a website or software. It then manipulates the end-user's computing device to validate cryptocurrency transactions. This process is called mining and earns digital currency for the attacker that may be used to fund future operations.

Hackers recently used the cryptojacking approach to hijack the computing power of visitors to several state and local government operated websites. This was done by inserting code into a third-party service used by the agencies targeted.

The technique of using third-party code to deliver a malicious payload is growing since it can quickly empower attackers with tremendous computing power. And the capability of this approach to cause large-scale damage was clearly seen in the attack as, over a four hour period, thousands of websites were infected and connected users impacted.

At first glance, cryptojacking might appear to be a relatively harmless form of attack since it is not encrypting your data and demanding a ransom. But the truth is, it can cause serious strains on your network resources by reducing available processing power, increasing energy usage, and quietly drawing your network into an illegal activity.

To learn more about the potential cost that cryptojacking can have on your agency's resources and finances, check out the latest Talos blog at:

http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

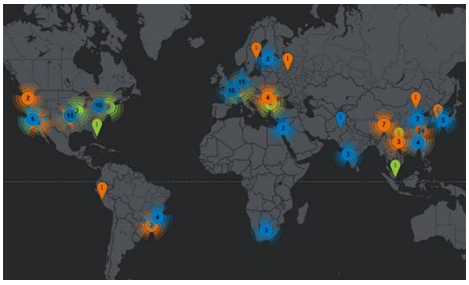
Operations and Citizen Services

The operation centers that manage the smooth delivery of daily services that citizens expect from government are now faced with a number of cybersecurity threats that, left unchecked, could dramatically and suddenly reduce quality of life in our nation. It is critical that the public sector be prepared to deal with these threats so that continuity of government is ensured and services vital to the public health continue.

Government must embrace strategies that promote continuity of services during times of crisis, especially those related to the health and welfare of citizens.

A small attack can have big consequences

The broader impacts a cyberattack, even a small one, can have on government are often overlooked. These include damage to key citizen services. Unfortunately, the political reality is that many who should be dealing with this are often distracted by political issues or merely unsure how to address it. And for operation centers that orchestrate the constant flow of data and communications touched by government or individual agencies, even a minimal attack can disrupt public and social services, healthcare, food aid, elderly assistance, and waste removal. This could jeopardize the health and welfare of our most vulnerable citizens.



To provide these services, government is increasingly sharing and storing massive amounts of sensitive constituent data such as Social Security numbers, healthcare records and driver's license numbers. The data is often available through networked systems in a centralized operations center that provides a unified view of an organization's data. But left unsecured, it could find its way into the hands of adversaries bent on abusing it for pain or profit.

Ransomware and third-party attacks

Ransomware, a form of malware, poses a particularly large risk since most agencies that provide direct services to the public usually rely heavily on email and website interfaces. Many public sector entities have already paid ransoms in an attempt save their data.

Montgomery County, Alabama paid nearly $50,000 to purchase nine bitcoins, a universal online currency, for attackers to get seventy terabytes of encrypted data released before it was erased (more here). This and other similar malware attacks against government operations and citizen services were likely triggered after a public employee opened a malicious email. But incidents like these can easily be reduced by ensuring software is updated regularly and proper patches installed. Also helpful is regular training for employees that instructs them on how to recognize potential malware in their email or on websites they may visit.

The need for continuous diagnostics and monitoring

Data breaches, even accidental by trusted vendors, can also leave public sector networks, and the private citizen data they store, exposed. This can happen when third-party code is inserted into software that vendors provide citizens for accessing government networks.

Continuous diagnostics and monitoring (CDM) is favored by the federal government and can reduce this threat by providing constant monitoring of networks and endpoints for suspicious activity, enabling deeper visibility into networks, and using automation to reduce remediation times. The Department of Homeland Security (DHS) has already started a CDM program at the federal level (learn more here).

Confronting the breach

Unfortunately, according to our study, Operations is the area most negatively impacted by breaches in government (41%). The biggest obstacles for government in adopting advanced security processes and technologies include budgets (34%), lack of trained personnel (29%), and lack of knowledge (26%).

A positive for government is in how agencies dealing with public scrutiny during an attack are responding. Over seventy-two percent are voluntarily disclosing the incidents, which can only serve to increase public trust in times of scrutiny. Ninety-one percent upgrade security after an attack. And over forty-three percent are doing this by investing in new cybersecurity solutions.

Utilities and Energy

The networks that control our energy grids, water purification systems, wastewater treatment plants and other critical infrastructure are increasingly complex. As they subtly merge into the Internet of Things (IoT), our nation's utility networks are empowered to scale wireless sensors and controls in extremely efficient ways. But this is also increasing the number of endpoints and opportunities for exploitation, making high profile, high impact targets even more attractive to those who wish to do our nation harm.

Government must move to better secure wireless technologies and provide greater resilience for their increasingly complex networks.

Targeted attacks and APTs

As utilities continue the adoption of wireless technologies to manage infrastructure, it is creating more complexity within their networks. But newer software technologies that sense, monitor, and actuate physical processes, often within machinery, without human intervention are becoming the standard. And when combined with security weaknesses within software running on their networks and endpoints, it is dramatically increasing the attack surface their security teams must protect. For the public sector, the integration of software and embedded systems into physical devices is increasing the challenges faced by security professionals in the utilities and energy industries.

Because of this, targeted attacks continue to top the list of worries for utility and energy security professionals, as do advanced persistent threats (APTs).

APTs have the potential to remain undetected in critical networks for longer periods of time, increasing the damage that attackers can cause.

With large and complex facilities such as water purification and energy production, this could lead to significant disruption of services.

Small or large, utilities are high profile targets

With the growing use of connected devices, increasing material costs, and a strict regulatory environment, keeping utilities secure can be a challenge for government, especially at the local level. This was the case for the small city of Spring Hill, Tennessee recently, when a ransomware attack disabled utility meters and also shut down their electronic payment system (more here). This affected the city's finances for several months and also left citizens, many who are on fixed incomes, owing larger one-time payments than they had budgeted for.

It was also recently revealed by the federal government that the nation of Russia had been pursuing an ongoing campaign of cyberattacks against U.S. infrastructure (more here). This included more than a dozen power plants in seven states, plus water treatment plants in several communities. These attacks appeared to be targeted and rolling; probing our infrastructure for weaknesses that Russia can exploit if future political incidents or military conflicts occur.

Stay secure through better standards, daily alerts, and regular drills

Energy Secretary Rick Perry testified before congress that cyber attacks are "literally happening hundreds of thousands of times a day. The warfare that goes on in cyberspace is real, it's serious" (more here). For utilities, this is difficult. They are a unique target for attackers because the impact their destruction can have is immediate and cascading. That's why adhering to industry standards is important.

In our survey, utilities report that using a standardized information security framework, such as ISO or NIST, is serving them well (59%) or very well (38%). But there is room for improvement for those getting daily security alerts as only fifty-five percent of alerts are being investigated. Fortunately, only thirty-four percent turn out to be legitimate.

We suggest security professionals should take the following action, aggressively, to protect our utility networks:

- Initiate automated processes to quickly mitigate alerts and better implement standards.
- Create more efficient responses to meeting regulations.
- Establish quarterly drills and simulations to detect weaknesses in security infrastructure.

Remember, the public recognizes that utilities are part of the critical infrastructure, and that breaches put key services, and citizen lives, at risk. So when utilities suffer public breaches, transparency on the part of government is important.

Transportation

Connected transportation is the buzzword for public sector agencies involved with vehicular, rail, port, air and even bicycle traffic. From light rail and autonomous vehicles, to hyperloops and hypersonic transports, the future is bright for creative alternatives to traditional transportation. But one common thread is connecting them all: wireless technologies.

Government must push decision making to the network edge, where data originates, to provide greater resilience in the face of attacks.

Consumers continue to drive security needs

In the past, technologies used in transportation infrastructure were closed systems. But today, the explosion in mobility, fueled by the IoT, has changed that. Open and integrated networks are needed to power transportation. And they must be accessible not only to government but to the citizens and private sector entities that will use them. This means more transparency, greater simplicity in access, and most importantly, stronger cybersecurity.

Mobile devices are now common place and consumers desire to use them to view real-time schedules, purchase tickets, access news and entertainment, and to receive alerts or report security and safety concerns.

Growing social networks for transportation can have thousands of endpoints attackers can use to get inside government networks. Add connected vehicles to the mix, and the potential for chaos may be significant.

To more quickly and securely meet these and other needs of citizens (including transportation employees using smartphones and tablets for their work), government should consider building secure, real-time mission fabrics that push decision making to the network edge, where data originates. With this approach, agencies can offer more secure services, improve efficiencies and lower costs, often without an expensive network rebuild.

This innovative new approach can help transportation agencies establish a foundation for secure and agile deployment of roadside services. And convert an existing network into a real-time automated and integrated network environment.

Budgets and benchmarks key to staying secure

As with most every area of government, a lack of security talent is proving to be a key challenge for security teams in transportation. Outsourcing can only serve as a temporary crutch. Agencies must increase their budgets for network security personnel so they can start recruiting, compensating and retaining the level of talent they need to keep secure.

Government agencies should also seek adherence to standardized security practices, such as ISO 27001 or NIST 800-53. And participate in a security standards body or industry organization, such as PT-ISAC or ST-ISAC.

Attack simulations helpful in preparing for the worst

Like energy production, transportation is a heavily regulated industry. This need to meet regulatory requirements can be of big benefit for government. How? By helping push the use of attack simulations to uncover weaknesses and better understand potential attackers' methodologies. Quarterly drills have been shown to drive significant improvements in security policies, procedures, and technologies and should be a best practice in transportation.

Ransomware still on track to dominate

Despite the advances made in cybersecurity, data breaches continue to be a major player. This was evident in a recent cyber attack that struck in Eastern Europe, affecting various mass transit. In the Urkaine, a ransomware identified as NotPetya, a variant of the infamous Wannacry ransomware, began encrypting files and demanding payment in bitcoins for their release. This attack impacted both Kiev's city subway and airport, where it altered electronic signage boards to display a ransomware note. And a ransomware called BadRabbit later struck the same region, impacting air travel that resulted in confusion among passengers and delayed flights (more here).

Our survey found that twenty-five percent of transportation organizations suffering a breach had their systems taken offline for more than an eight hour work day, eventually impacting twenty-three percent of their entire network. Lastly, sixty-four percent of the breaches involved a law enforcement response. As a result, transportation security professionals stated that being the victim of a breach continues to be a driver of improving security, with over twenty-eight percent saying it did so to a great extent.

Public Safety

In times of crisis, first responders benefit greatly from the greater situational awareness that collaborative technologies can provide. Real-time video and information sharing, reliable and secure IP communications, and ruggedized routers that can extend their mission fabric are key to saving lives and maintaining quality of life during both natural and man-made disasters. And, unfortunately, our adversaries know it.

Government must seek an end-to-end cybersecurity approach that protects mobile assets, even as mission fabric is actively scaled.

Targeting those who serve us every day

Public safety agencies across the U.S. are continually under attack by cyber criminals (more here). From small towns and large cities, to military bases and university campuses, the desire to harm those who protect and serve, continues to grow. This was the case in the small township of Mad River in Ohio, where data containing private citizen information was encrypted and a demand for ransom issued. In the end, several years of data that was stored on a server in its Fire and EMS station was lost due to the breach (more here).

For a suburban Dallas police department, eight years of digital evidence (including for an active criminal case) was lost after a similar attack. And in Murfreesboro, Tennessee, the city's emergency services were targeted, and data permanently lost. But adversaries can also attack the very equipment used by public safety agencies. The use of IP cameras, motion and environmental sensors, smartphones and tablets are now common among public safety personnel. Ruggedized vehicle mounted routers are also becoming the norm. In times of natural or man-made disaster, as well as every day, these technologies can do great things (learn more here), but they do need to be secured against attack.

Ransomware continues to wreak havoc

It is clear that ransomware continues to be the most popular method of attackers bent on damaging our nation's law enforcement, EMS, fire and rescue services. It will attack your organization by various means, including already known vulnerabilities left unfixed, by attaching to files, or by using backdoors. Unfortunately, even if a ransomware attack is not completely successful, it can harm something just as important as data: your reputation. When an adversary strikes, government must mitigate more than just the damage to their network, including:

- Inability to properly deal with emergencies, resulting in damage to property and the potential loss of lives.
- Damage to ongoing investigations/prosecutorial cases.
- Increased scrutiny from political leadership that could negatively impact personnel and budgets.
- Media coverage that can damage relationships with the public and other agencies.

Paying ransom feeds the beast

Unfortunately, the adversaries behind these threats are taking their malware to an entirely new level of effectiveness by using cryptographically sound file encryption. This technique prevents the majority of ransomware from being easily decrypted. This new twist might leave your agency tempted to pay the ransom, but remember there is no guarantee you will be able to decrypt your data afterwards. Attackers may have also planted hidden malware during the initial attack phase that will be activated later. In addition, by paying ransom you become an active part of the problem, helping fund development of the next generation of ransomware.

Adopting a cybersecurity framework that lowers risk

To help public safety agencies in the United States stay more secure, the FBI and National Institute of Standards and Technology (NIST), have used their own experiences to create best practices for cybersecurity. These can be used as an introduction to methods for securing your own agency:

- The NIST Cybersecurity Framework is a collaborative effort by both the private sector and public sector that provides a common language to address and manage cybersecurity risk in a cost-effective way, without placing additional regulatory requirements on organizations.
- The FBI's Criminal Justice Information Services (CJIS) Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. Developed primarily for courts and law enforcement, other public safety agencies may be able to leverage its best practices to simplify operations, increase efficiency and speed processes.

Education

Those in education must strike a delicate balance between safeguarding personal data and intellectual property while encouraging creative teaching, learning, and engagement. But the increasing use of IoT and BYOD in education is opening up opportunities for adversaries, most notably in higher education, where more than half of respondents (fifty-eight percent) in the 2018 Security Capabilities Benchmark Study reported experiencing at least one public security breach in the past year.

Government must secure educational networks, and the rising number of devices connecting to them, from targeted attacks, especially those coming from the evolving use of an old nemesis: ransomware.

The proliferation of IoT and BYOD on campus

It's not surprising that those in education point to the proliferation of BYOD and smart devices as a critical security challenge. On most campuses, smart devices already outnumber traditional computing equipment. Consider students who rely on smart watches, wireless speakers, personal assistants (and game systems) in addition to their smart phones, tablets, laptops and printers.

At the same time, schools, colleges and universities deploy thousands of smart devices themselves, from video surveillance equipment to parking systems, and from wayfinding technology to smart laundry or vending machines. And adversaries are increasingly exploiting security weaknesses inherent in IoT devices like these to gain access to critical systems. This often involves using IoT botnets to launch DDoS attacks that are increasingly broad and intense.

More than seventy percent of higher education respondents to the 2018 Security Capabilities Benchmark Study feel IoT and BYOD devices pose a high or moderate risk for their campus. For security personnel in education, they are perceived as the most challenging area to defend. As a result, twenty-nine percent say they have already experienced a cyber attack on operational technologies (OT), while sixty-five percent say they expect one this year.

Increasing concern about ransomware

The threat to education from ransomware, especially colleges and universities, is evolving as adversaries eliminate the human element and use "automated" network-based ransomware cryptoworms to attack. Seventy-five percent of higher education respondents report they understand ransomware's potential danger and feel it poses a high or moderate risk to their organization. Twenty-nine percent feel it is their greatest concern.

Security personnel in education also report a growing fear of advanced persistent threats (41 percent), targeted attacks (36 percent), and concerns over the proliferation of smart devices (36 percent). They're right to be concerned. Some adversaries who would launch this new generation of ransomware don't actually care about collecting a ransom; their goal is more insidious: the complete destruction of the systems and data they infect.

The lack of budget and cybersecurity specialists

Budget constraints (41 percent) and a lack of trained personnel (21 percent) are among the top challenges facing security specialists in education. Colleges and universities report employing an average of twenty dedicated security employees, half that of most industries. This notable shortage of security personnel results in a lack of proper threat investigation and remediation. It is also hindering the deployment of innovative technologies or processes that could strengthen their security posture. But respondents do understand the value that increased staffing could bring and would use those resources to expand cloud/mobility security, network forensics, and data protection capabilities.

A real and costly threat to learning

Any security breach at a college or university can have serious implications: from legal ramifications of violations to FERPA or CIPA, damage to an institution's reputation, lost productivity, and significant financial costs. But more importantly, it can take time away from teaching and learning. Forty-nine percent of respondents report their systems had been down for nine hours or more as a result of a recent security breach. Thirty-two percent of these indicated that more than half of their systems had been impacted. Also worth noting, about half (51 percent) of attacks resulted in financial damages of more than $500,000 with an additional twenty-three percent reporting losses between $100,000 and $499,000.

National Defense

Innovative technologies related to cloud, big data, the IoT and mobility increasingly play a critical role in keeping our nation safe. They also generate additional network traffic and its inherent security risks, straining Department of Defense (DoD) legacy networks. This can limit the joint forces' ability to effectively and securely complete critical mission objectives. But a modern IT infrastructure can empower the DoD to deploy the latest threat detection.

Government must seek a security based modernization of defense networks to better confront threats, both physical and cyber, to keep our nation safe.

The need to simplify, strengthen and embed mobility

Cyberspace is playing an increasing role in how wars will be waged in the 21st century. The modern U.S. military now relies on cyberspace to conduct critical exercises: everything from tracking force and enemy movements to linking and gathering data across weapon systems and battlefield platforms, including aircraft, drones and robots.

Although the digital and cyberspace domain has enhanced the military's mission capability, it has also created a complex national security environment more open to cyberattacks. "Unfortunately, the current DoD network is too complex, fragile, not sufficiently mobile nor expeditionary, and one that will not survive against current and future peer threats, or in contested environments" according to Lt. Gen. Bruce T. Crawford, Army CIO, during recent congressional testimony (more here). "We find ourselves in a position now, within a new environment and facing new challenges, where our network is not user-friendly, intuitive or flexible enough to support our mission."

To compensate, the DoD has turned to industry vendors to fill the gap as standard government acquisition processes haven't kept up with the commercial innovation explosion. Plus the DoD can be a difficult environment to navigate. But to confront new cybersecurity threats, it will have to reconsider the way it operates, turning its focus further towards agility, collaboration, consolidation and informed decision-making (learn more here).

IT modernization and behavioral analytics key

To stay secure, the DoD must consider a security-driven network refresh to replace outdated equipment. This can help eliminate vulnerabilities and mitigate risks, while allowing the joint forces to take advantage of the efficiencies and functionality of new technology. This IT modernization should include network-embedded, context-based security that reaches from the enterprise to the tactical edge, driven by increased automation, behavioral analytics (machine learning and artificial intelligence), and next generation encryption (learn more here).

Keeping physical facilities secure

For the DoD, cybersecurity also extends to physical facilities. Facility related control systems (FRCS) is a mission-critical function that focuses on control systems associated with real property, including functions like HVAC, power management, backup power, elevators and escalators, and life safety systems. These assets, and the functions they serve every day and in times of crisis, are especially important to protect because their failure could impact critical mission activities, pose security threats, and result in hazardous environments.

An incorrectly designed or maintained FRCS could also create network gaps that adversaries could use to access other, more sensitive areas of the DoD. Deploying a proven cybersecurity framework that features threat intelligence, detection, and protection at every node is critical in this case. This would allow trusted devices to serve as sensors and enforcers to implement access policies, segmentation strategies and remediation actions, increasing the resiliency of our nation's physical facilities to attack (learn more here).

Moving towards a more real-time security posture

The DoD can also improve their security posture by adopting technologies that can increase visibility into their network and do so in real or near real-time, plus:

- Deploying a standards based, security architecture.
- Better authenticating network access and security postures of users to prevent spread of malicious software.
- Using sensor and telemetry data for deeper visibility into their networks, connected devices, and user activities.
- Continuously monitoring network and user activities via anomaly detection and machine learning.
- Automating response to attacks.

2018 Recommendations for defenders

As the impacts on government from cyber attacks continue to rise, it is becoming more clear that those responsible are doing so to purposely damage both public services and infrastructure. More alarmingly, they may be committing many current attacks in an attempt to learn which strategies will inflict the most damage and what our defenses are, all in preparation for larger, more devastating attacks. So those involved in public sector security must ask: Are we sufficiently prepared, and are the networks we manage resilient enough to survive?

To keep public sector networks secure, government must continually adapt and respond to current and emerging threats by adopting innovative technologies and processes.

Stay agile, adapt and get creative

Based on findings from the Cisco 2018 Security Capabilities Benchmark Study and events of the last year, we see that defenders have many challenges to overcome. Fortunately, there is a clear and growing understanding of the issues by public sector security personnel. Coupled with a more holistic, threat-centric approach and adhering to best practices for cybersecurity, a strengthening of resilience in the face of attack can be achieved across all levels of government.

In addition, by focusing on strategic security enhancements that provide end-to-end security with deeper visibility, government agencies can better defend public services and infrastructure. To achieve these goals, the public sector at all levels, from state and local, to federal and education, should consider the following recommendations.

- Implementing first-line-of-defense tools that can scale across networks and devices, like cloud security platforms.
- Adhere to security policies and best practices for application, system, and appliance patching.
- Backing up data often and testing restoration procedures/processes.
- Adopting next-generation endpoint process monitoring tools.
- Using network segmentation to help reduce outbreak exposures.
- Accessing timely, accurate threat intelligence data and processes that allow for that data to be incorporated into monitoring and eventing.
- Performing deeper and more advanced behavioral analytics.
- Reviewing and practicing security response procedures, including through simulations or drills, on a regular basis.
- Requiring third-party vendors or app developers to meet more stringent security requirements.
- Conducting security scanning of microservice, cloud service, and application administration systems.
- Reviewing security systems and exploring the use of SSL analytics and, if possible, SSL decryption.

Conclusions

In the public sector threat landscape, adversaries are increasingly adept at evading detection when attacking networks. They have shown the capability to damage public services and infrastructure by weaponizing the very technology that benefits our society as a whole. They are attempting to do this by destroying sensitive data or holding it for ransom at every level of government. Or by taking critical infrastructure for utilities, transportation, public safety, and defense off-line. Unfortunately, our adversaries are often funded by hostile nation-states or shadow organizations, giving them more effective tools and tactics to achieve these goals.

Government must increase resilience from attacks by adopting an end-to-end, threat-centric cybersecurity approach that provides deeper visibility into networks.

Achieving victory in the growing cyberwar

As adversaries increase the tenacity and occurrence of their attacks against the public sector, it is important for those in security leadership positions to actively stay educated on emerging methods that may be used and how to prepare their defense against them. By better understanding their adversaries before they strike, government can better protect public services and infrastructure. And it will enable agencies to better secure agency and private citizen data. But this should involve strategies, using both technology and the people behind it, that increases the resiliency of government in the face of attacks.

Over the past year, it has become clearer within the threat landscape of the public sector that there is a need to adopt end-to-end, threat-centric cybersecurity approaches that provide deeper visibility across networks. Doing so can greatly improve the security of private citizen data and provide a more secure environment across the entire attack continuum. This helps government:

- Better prepare for attacks before they happen.
- Mitigate attacks faster as they unfold.
- Remediate attacks more thoroughly afterwards.

By building a "cyber resiliency" into government networks, the public sector can withstand attacks that may have otherwise created significant damage.

As the public sector moves towards this goal, it should seek greater adoption of cybersecurity frameworks based on national standards and guidelines. By using existing, proven best practices, it can efficiently and more affordably secure networks. This should also involve a more holistic approach that also moves cybersecurity to the network edge where a more proactive defense can be staged.

How Cisco can help secure the public sector

Cisco delivers intelligent cybersecurity for governments at all levels, including state, local, federal and education. We provide one of the industry's most comprehensive advanced-threat protection portfolios of solutions across the broadest set of attack vectors. Our threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Cisco Collective Security Intelligence (CSI) ecosystem bring together the industry's leading threat intelligence for the public sector, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open-source community. This amounts to a daily ingest of billions of web requests and millions of emails, malware samples, and network intrusions.

Our sophisticated infrastructure and systems consume this telemetry, helping machine-learning systems and researchers track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, and email, and from the cloud, to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered to our partners in the public sector.

To learn more about our threat-centric approach to security, visit cisco.com/go/security.