WHITE PAPER

Government Cyber Security
Responding to Rapidly Evolving Threats.
How Government Agencies Can Better Respond to Constantly Changing Threats

Government Agencies and Their IT Assets Are Under Attack

The data security and IT integrity of local, state and federal government agencies are under unprecedented attack. A startling increase in the sophistication and number of cyber attacks is forcing virtually every agency to rise to a level of security consciousness that would have seemed excessive or even paranoid just a few years ago.

That was then, before the words “phish,” “WikiLeaks,” “spam,” “virus,” and “Trojan” acquired new meanings and became part of everyone’s vocabulary. This is now. Government departments have recently experienced a serious run of data breaches. We all know the big headlines, but, as revealed in a report from the Center for Strategic and International Studies (CSIS), there are many serious incidents occurring beneath the public’s radar screen. Highlights since 2014 include:

- The IRS getting hacked, resulting in a $50 million loss – blamed on Russian hackers.¹
- Russian hackers penetrating the Department of Defense (DoD) unclassified network.
- US Postal Service servers getting hacked, exposing employee names, addresses and social security numbers.
- The State of Maine and Fort Lauderdale, Florida’s sites being taken down by hackers.
- The Department of State’s unclassified network and email system being breached and closed down by hackers.
- Internationally, the governments of Saudi Arabia, The Netherlands, South Korea, Canada, India and Finland being attacked, often with serious data breaches and other damage to data assets.

It may be tempting to disregard international incidents as irrelevant, but that would be a mistake. Cyber risks flow across borders. In the case of India, it was actually an attack on the French shipbuilding company DCNS that caused the breach of secret designs for India’s new Scorpene submarines. DCNS also makes submarines for Chile and Malaysia. A vulnerability in one country can expose other governments to cyber risk.

Today, with so many potential attackers, it’s hard to draw up a reliable short list so that you can start the process of planning your defensive strategy. It’s even harder to thwart an attack if you don’t know what an attacker might be trying to achieve. Is someone launching a distributed denial-of-service (DDoS) attack to shut you down for a few hours and create uncertainty among your constituents and other stakeholders? Or is that just a smokescreen for stealing (or modifying) government data?

It can be difficult to determine what’s motivating the attack. Sometimes, it’s about money but with government hacks, the purpose is often more about power, image and influence. They may be seeking to cause damage for their political benefit. Attacks might be driven by nihilism, ideology, bragging rights, or a host of other motives. Vikingdom2015, the hacker who shut down Maine’s site with DDoS, claimed he targeted Maine “because they were dumb.”² Increasingly, we seem to be seeing cyberattacks as acts of aggression, more or less, coming from extremely well-resourced foreign entities.

Just as the landscape of potential attackers and motives keeps changing, so too does the arsenal of disruptive tools and techniques available to them. Today’s adversaries are more sophisticated than ever before, with access to more code and expertise than existed just a few years ago. It’s not enough for your organization simply to thwart an attack: you have to continually prepare for the next one even though you can’t predict much about it — except that it’s likely to be smarter and stronger than the one you’ve just survived. You need to build up a dynamic and proactive defensive capability that protects you from attack and increases the speed and agility of your response to any threat.
Raising the Drawbridge is Not an Option

Government agencies are typically outgunned by the hackers. Attacks are bigger and more sophisticated, and perimeters are more permeable than ever before. As Booz Allen observed, “The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber-attack, as each creates another vulnerable access point to networks.”

It’s tempting to imagine walling off all government systems, but current practices won’t allow it. Cloud, social, and mobile technologies, including “Bring Your Own Device” (BYOD), are simply too cost-efficient and effective for government organizations to ignore. And, your constituents expect easy access. According to Pew Research, 49% of all adults have accessed government websites at the local, state and federal levels. This figure has risen every year. Today, government mobile apps are becoming a bigger part of the picture. There’s no retreat from the levels of openness and access that citizens have come to expect.

Your Organization Has Already Been Infected

These days, every organization must base its security strategy on an acceptance that it is already “infected” with some form of malware, to some degree, with or without knowing it. Because perimeters must be permeable to allow web server traffic to flow and employees to interface with the public and vendors, complete protection is impossible. Traditional defenses are still useful for blocking and tackling to defense in depth. But you have to augment them by dealing with attack mechanisms that have infiltrated your organization. You need to shift the focus of cybersecurity tactics from building walls to analyzing, detecting, and expunging threats already inside your system. How can those be identified, stymied, and removed?

Due to the complex kaleidoscope of attackers, motives, and tools, these are difficult questions to answer. Yet, regulators — and your political sponsors — are going to be holding you responsible for doing so. This is a lot of responsibility for an agency to shoulder. The mitigation of security risks has become such a complex task that it’s much like a totally separate area of activity. The question arises: Do you want to be in the cybersecurity business? Is state-of-the-art IT security a specialty that you want — or can afford — to build in house?

“High-profile data breach events have hastened stakeholder focus on the ways in which sensitive data is housed and whether management is taking a holistic and comprehensive approach to protecting the data.”

- Bloomberg Law Reports
What is the Next Attack?

Today’s threat environment comprises more attackers — and more tools — than ever before. It’s impossible to describe all the tools and other resources that may be used to launch an attack on your organization, because the scope is expanding all the time. Criminal enterprise supply chains sell inexpensive software tools that can be quickly customized to suit the attacker’s goals and avoid detection by systems. Commercial DDoS attack services and DDoS bots that combine high-volume bandwidth and low-volume application-level attacks are readily available and can be used to shut down your online services — and can also serve as a distraction while a more focused and stealthy attack takes place on your organization or on another organization that uses the same ISP. Public websites that your staff visits can be infected in a way that specifically targets your organization. Well-crafted spear-phishing emails can hook even senior and savvy employees. And new “bots” are continually evolving to be smaller, harder to detect, more effective, and more organized, making them impossible to flush out of systems.

Where is the Next Attack Coming From?

This continually evolving arsenal of tools is in the hands of a wide range of attackers, from shadowy organizations and individuals such as nation-states, criminals, hacktivists and terrorists, to the most damaging attackers of all — well-known and even well-liked insiders. In the case of the government, one of the worst attacks ever, the Wikileaks theft of classified diplomatic cables, was carried out by an insider.

Nation-States

Recent news has highlighted the cyberterrorist activities of nation-states motivated by political and ideological differences. Iranian terrorists carried out cyber-attacks on nine of the US’s leading banks using data networks or clouds — like those run by Amazon and Google — as well as a host of smaller companies. Suspected Russian hackers attempted to penetrate the Turkish Prime Minister’s office and the German Democratic Christian Party in 2016. (CSIS) Saudi Arabian military systems were also hacked in 2016, with suspicion falling on Iran.

Cybercriminals

Criminals are everywhere — and cybercriminals are also nowhere, making them virtually impossible to catch. The Duanesburg School District in New York State lost $3 million to hackers, for instance. Young hackers are being offered large sums of money — and bragging rights — in exchange for taking on the challenge of bringing down major institutions. As one example, a cybergang thought to be based in Eastern Europe and the former Soviet Union is recruiting dozens of people to participate in a scheme to steal millions of dollars from 30 major U.S. banks, according to RSA. The organizers are thought to be associated with the Hangup Team, which claims to have used a proprietary Trojan family, called Gozi, to siphon $5 million through online banking accounts since 2008. This is just one example. There are likely to be many more such gangs in operation.

Hacktivists and Cyber-Terrorists

Hacktivists and cyber-terrorists, some sponsored by nation states and others working only for themselves or small groups, are motivated mostly by the desire to disrupt political stability. The hack of the Democratic National Committee in 2016 falls into this category. Security organizations track pending campaigns, and warn that some of the threats on the horizon could be devastating to financial services firms. Project Blitzkrieg, for example, is a “credible threat” according to McAfee Labs, because though it hasn’t yet infected thousands of victims, the attackers have managed to run an operation undetected for several months while infecting a few hundred businesses. This attack combines an innovative technical backend with the tactics of a successful, organized cybercrime movement. Rather than launch a sweeping attack, McAfee said the campaign selectively targets accounts at investment banks, consumer banks, and credit unions, because doing so makes it easier for attackers to evade network defenses.

Today’s Threat Landscape

- 111,111 unique strains of malware deployed every day
- 10,000 malicious new domains deployed every day
- 1,100 DDoS attacks launched every day
- 4759 Gbps peak attack (just one recent example)
- 1,057 active botnets
Insiders
Insiders include current or former employees, contractors, or other business partners who have or had authorized access to your network, system, or data. Because they can bypass your security measures through legitimate means, they can misuse that access and knowledge to impact the confidentiality, integrity, or availability of your information or information systems. Privileged access enables insiders to inflict more damage than almost any other attackers. Sometimes, they do so unintentionally, through error or carelessness. But if managers in organizations set out to commit fraud or mischief, studies show that their schemes tend to cost organizations twice as much as when non-managers instigate these crimes.

What Does an Attack Cost You?
Attacks can be very expensive to remediate. The data breach at the Federal Office of Personnel Management (OPM) is projected to cost $330,000,000 to fix. It’s the same in the corporate sector, with Target facing an expense estimated to reach $1 billion to make up for its massive breach. For smaller companies, a successful DDoS attack in the corporate sector might cost $150,000. But attacks can be even more damaging in ways that are less easy to measure.

Your agency’s credibility and public trust suffers when customers experience down time as a result of a DDoS attack. There can easily be political fallout because a bad security incident can cause popular backlash against elected officials. Productivity takes a hit as well, as highly-paid employees are forced to idle, waiting for service to be resumed. Data in the private sector bears this out. In a recent survey, 70% of small-to-medium business who had experienced a single instance of fraud reported diminished confidence; approximately 40% closed their accounts and switched to other financial services providers.

What Can Your Agency do for Itself?
Like most government agencies, you have probably already taken extensive precautions in house. You’ve almost certainly locked down applications and servers, configured perimeter firewalls to block network attacks, and implemented as many of the other 30 or so security best practices set out in various websites as you could afford to do.

But is that enough?

In every sector, government organizations are asking the same question — and in the high-profile public arena of government, the question is even more urgent. Increasingly, agencies are weighing the merits of buying IT security services, rather than trying to build (and maintain) their own. Today’s constantly changing landscape of threats and rapid evolution of new technologies make it difficult for most agencies to fend off attacks. Leveraging the scale and — most importantly — the expertise of IT security services providers offers your organization a way to gain higher-quality protection, more cost-effectively, than you could do on your own.

Buying IT Security as a Managed Service
Depending on the provider and package, buying IT security as a managed service can provide your agency the hardware, software, infrastructure, and — most critically — the information and expertise that you need to protect your organization in today’s complex and evolving threat environment. This is not a complete list, but it does cover some of the most important — and some less well-known — security issues to consider.

DDoS mitigation services should be at the top of your list of required services. Consider only those providers who can detect attack traffic on their or your network before it impacts your infrastructure. Providers should be able to divert traffic and cleanse it of malicious packets before forwarding it to your site. Services can be expensive, so look for one that charges only a low monthly “retainer fee,” plus an hourly charge for traffic cleansing, so you get protection but don’t
You’ll also want one that commits fully to standing by you in case of an attack, with skilled analysts who not only monitor the network for attack traffic, but also work with you around-the-clock during an attack to deploy any available countermeasures to keep your site protected.

Web application protection can help your organization to cost-effectively protect sensitive information from application-based attacks by detecting and blocking malicious web requests, learning the expected usage and monitoring activity of protected applications, and inspecting outbound traffic to ensure no data leakage — all with minimal latency.

Cloud computing security services are essential for your hosted or internal cloud. Your provider should secure your data through encryption and masking but allow you to remain in control of it. In order to buffer your infrastructure from the dangerous world that exists beyond your network, the provider should proactively identify attacks that can pose the greatest threats to your highest-value IT assets, filter out insignificant attacks so you can focus on the more critical ones, and continually scan for internal vulnerabilities.

Log management may not seem like a front-line security issue, but it is important as the volume of log data you accumulate increases and as compliance requirements proliferate. There’s a lot of work involved in collecting, analyzing, and archiving IT logs. Look for a service that can cost-effectively assist your organization in addressing its compliance requirements, such as the PCI DSS requirement that any entity that processes credit card data must securely gather, analyze, and archive specific log data, making it available online for 90 days and archiving it for 12 months. And to help you get value from that data, it should also provide an easy-to-use interface that includes a broad range of standardized reports as well as the ability to customize reports to meet your specialized requirements.

Network intrusion detection and prevention can help you keep pace with the growing volume of increasingly complex cyber-attacks. Look for a service that will alert you when a critical threat that might have a significant impact on your security infrastructure appears and respond around-the-clock with appropriate action based on your preferences. Even when no threat is on the horizon, you should seek a service that configures, monitors, and maintains Intrusion Detection and Prevention (IDP) sensors, and provides ongoing detailed monitoring and reporting for a better view of potential problems and vulnerabilities.

Content integrity monitoring too often flies under the radar of internal security groups. But with some attacks focused on tampering with data in files, you need a service that helps you keep a constant watch on your mission-critical files and programs. Look for one that monitors critical directories and files residing on a host computer and alerts you whenever specified files undergo an unexpected change.

A State-of-the-Art Solution: CenturyLink Managed IT Security Services

CenturyLink offers all the state-of-the-art services described in this paper — and more. Whether you want security protection delivered at your premises, within a CenturyLink data center, or “in the cloud,” we’ve got you covered. Our services range from a basic firewall to comprehensive security coverage that includes threat management, DDoS attack mitigation, log monitoring, web application protection, authentication and authorization services, and physical data center security.

When you select CenturyLink as your managed security services provider, we enter into a partnership with you, helping you assess your organization’s unique risk profile and threat landscape, spelling out the protective measures available to you, and then working with you as you decide which security tasks you’d prefer to handle in-house and which you would like us to take on.

No matter which path you choose, you’ll be able to tap into the unmatched range of skills of our security team. Security is not a sideline for us: it’s the heart of our business, and we invest in it accordingly. We have staff focused exclusively on network security, physical data security, infrastructure, law enforcement, national security, fraud management, enterprise technology protection, and enterprise security. We also work with numerous state and local government departments throughout the United States.

Specialists in each of these areas interact to gain fresh perspectives on current, emerging, and future threats to our clients. In addition, we are engaged in state-of-the-art information sharing and technology through public-private partnerships, including the FCC Communications Security, Reliability and Interoperability Council (CSRIC), and with the Department of Defense, Department of Homeland Security, FBI, and The White House.
Government organizations worldwide must take responsibility for protecting cyberspace, and information sharing among these organizations is likely to grow, particularly following President Obama’s announcement of an executive order to improve the nation’s cybersecurity. CenturyLink is positioned to be a key player in any such initiatives. The CenturyLink infrastructure includes more than 50 data centers in North America, Europe, and Asia, serving more than 1,500 enterprise security clients and hundreds of financial services clients. With more than 5,000 security installations under management, and a track record of more than 20 years of delivering security, we have unparalleled expertise in cybersecurity. And, unlike some vendors, we are completely technology agnostic. We adopt only best-of-breed products to address emerging threats.

Can You Afford State-of-the-Art Security? Can You Afford not to Have it?

To deliver the security constituents expect today requires expertise and resources that not every agency has in house. If you wanted to create state-of-the-art security in house, just keeping your equipment and software current would take up a huge share of your total IT budget. Security technologies are expensive, and constantly changing. But that’s not enough. You would also need to find — and recruit and retain — skilled security professionals. These people are rare, and charge a premium for their services. You might choose to turn to your partners and third party providers for assistance with security, but unless you can be certain of every member and every system within that larger ecosystem, you could be increasing your company’s vulnerability rather than decreasing it.

CenturyLink has the scale and resources to provide the world-class security your agency needs in order to sustain its operations in today’s ever-changing and darkening threat environment — all at a commodity price. Call us today to start the conversation about how CenturyLink Managed Security Services can help your organization protect itself — and its customers — from evolving internal and external threats.

CenturyLink Infrastructure by Numbers

- 50+ data centers in North America, Europe and Asia
- 1,500+ cybersecurity clients
- Hundreds of government clients
- 5,000+ security installations under management
- 20+ years of delivering security