GOVERNING
IN THE AGE OF
CYBER THREATS

A PRACTICAL APPROACH
to safeguarding public systems and data
Governments around the world are working to meet citizens’ growing expectations for more and better digital public services. Across postal and revenue, policing and social services, or defense and back-office administration, digital technologies are fueling incredible innovations.

Platform-based ecosystems for connecting everyone involved in delivering services. Mobile apps for empowering citizens and government workers. And unprecedented personalization of online citizen experiences—all aimed at greatly improving outcomes and satisfaction with our governments, the services they provide and our interactions with them.

Yet the same technologies that enable these better services and enhance citizen experiences also contribute to cybersecurity risks. Whether originating from inside a government agency or from an actor on the other side of the globe, cyber threats are real, they are growing in number and complexity and, unfortunately, they are here to stay.

Every government agency operates with a unique mission—often with a constrained budget and limited resources. In the face of those realities, how can government effectively and efficiently safeguard systems and data? Success lies not only in investing in the latest security technology, perimeter protection, or monitoring services—though these all have a role in a cybersecurity program. Success also lies in developing and instituting a practical, proactive approach: Assess the risks. Build a flexible strategy. Engage the blend of technical and government expertise essential to staying ahead of emerging risks.

**DRIVERS OF CYBER INSECURITY**

Recent analysis suggests that public service organizations are a particularly desirable target for breaches and other cyber-attacks. Indeed, 50 times more attacks were launched against government targets in the past year than in any other industry.¹

The 2015 breach of the U.S. Office of Personnel Management (OPM) provides one of the highest-profile examples in recent memory. The two-pronged attack, executed by foreign state-level actors, started by gaining access to privileged user credentials and network architecture information that later made it possible for the hackers to gain access to portions of 20+ million personnel background investigation files for U.S. government employees.²

**50 times more attacks were launched against government in the past year than in any other industry**
The OPM breach is hardly unique; in the U.S. alone, healthcare provider Anthem suffered a similar breach, while the Internal Revenue Service has been targeted by foreign state-level attackers. Cyber-attacks have affected other governments around the world, as well. For example, in 2014, Canada’s National Research Council—which worked with more than 20,000 firms and research centers in Canada and globally—suffered a major breach of its network. The Canadian government blamed China for the breach, marking the first time that government had called out a foreign state for such an attack. In another example, documents and emails from Kenya’s Ministry of Foreign Affairs were stolen and then posted online by hackers in 2016.

**Cyberattacks have affected other governments around the world**

Though it is seen as a particularly desirable target, government is not alone in facing threats to data security and business continuity. In fact, a recent Accenture global survey of 2,000 cross-industry security executives revealed that roughly one in three targeted breach attempts against their organizations succeeds. Consistent with other surveys, 51 percent of these respondents admitted it takes “months” to detect successful breaches, while another 17 percent identify such attacks only “within a year” or longer. They also reported that internal security teams discover only 65 percent of effective breaches, with employees, law enforcement and “white hats” (that is, “ethical” hackers) finding most of the rest. With many security breaches taking hundreds of days to be discovered, this all demonstrates the level of challenge faced by government, citizens and businesses in securing the digital world today.

**ONE IN THREE** targeted breach attempts succeed (among the 2,000 organizations surveyed).

**51 PERCENT** of those survey respondents admitted it takes “months” to detect successful breaches.

**17 PERCENT** of those surveyed identify targeted breach attempts “within a year” or longer.
TODAY’S HOT LIST

Security breaches can come from numerous sources inside and outside an organization, and threats are nothing if not diverse and dynamic. Just when an organization believes it can successfully defend against one type of attack, another attack technique or vector emerges. Though risks are always changing, here are some of today’s most pressing:

RISE OF RANSOMWARE. In one flavor of ransomware, attackers send “phishing” email messages to government employees. When a worker clicks a link within the message, the computer is rendered unusable until a ransom is paid. In another variety, ransomers send a government agency a letter threatening to take down its network unless a ransom is paid (typically using the Bitcoin currency). In 2016, a campaign using “Locky” ransomware targeted organizations around the globe but mostly in the U.S., Japan and South Korea. Hospitals—with their life-and-death reliance on systems and data—were particularly hard hit.

In 2017, the “WannaCry” ransomware attack affected an estimated 200,000 organizations in 150 countries world-wide, locking-up the data of factories, hospitals, shops and schools across the world, and sending security companies scrambling to develop urgent fixes wherever possible. The very rapid spread of “WannaCry” globally was largely down to it affecting outdated Windows systems that are no longer security patched by Microsoft, a major security vulnerability known for years to have a disproportionately-large effect on public-sector organizations due to the very large number of users and less-frequent replacement of old systems.

INTERNET OF THINGS (IOT) SECURITY. A growing number of “things”—from cameras to coffee-pots—are going online. But with IoT devices, security often has been an afterthought. That can leave government-owned and—operated IoT devices vulnerable to breach. Today, there is the growing prospect of IoT devices being taken over and transformed into a “bot” to effect ever-greater damage. This technique was demonstrated in October 2016, when hackers hit infrastructure provider Dyn, which serves as a switchboard for Internet traffic. Using malware to harness webcams, digital recorders and other common connected devices, the complex attack caused outages that started in the eastern part of the U.S. and spread across North America and to Europe—striking prominent websites, including PayPal, Spotify and Twitter.

CLOUD SECURITY. For many governments, moving systems and data to the cloud is helping increase agility and contain costs—indeed, this was given prominence as early as 2011 when the Obama Administration’s “cloud-first initiative” pushed the US government to move core capabilities and services to the cloud. Yet, cloud computing must be undertaken with a careful eye toward security threats and risks. Citizens seem keenly aware of the potential for both great new opportunities provided by the cloud, and the potential dangers these present. In Accenture’s Global Public Service Citizen Survey, three in four respondents indicated they are concerned about cybercrime, with half saying that concern about cybercrime limits their use of online services, many of which are being moved to the cloud today. This high level of citizen awareness underscores the need for careful and disciplined security planning as part of every cloud implementation.

MOBILE THREATS. With smartphones in so many citizens’ pockets, these devices have become a valuable channel for engaging citizens and delivering public services. However, options are still limited when it comes to strong authentication and data encryption for most mobile devices. That presents a real risk if a device is stolen. What’s more, like laptop and desktop computers, mobile devices are gateways to users’ and organization’s data holdings—making these also vulnerable to various malware, including ransomware, deployed against connected mobile devices.
WHAT’S NEXT?

When it comes to cybersecurity, the “hot list” is a moving target. Innovation is constant, and as new technologies—from artificial intelligence to blockchain—emerge on the scene, new risks and new threats will crop up, too.

INDUSTRIAL INTERNET OF THINGS/INDUSTRIAL CONTROL SYSTEMS. Connected devices are gaining ground—and introducing new risks—in a host of industrial and infrastructure settings. As power plants, transportation systems and other providers of state-run infrastructure adopt IoT-enabled capabilities, governments need strategies and plans for ensuring the continuity and security of their vital resources. This lesson is well-illustrated by repeated hacking attacks against the power grid and military resources in Ukraine. In December 2015, hackers hit Ukraine’s Ivano-Frankivsk region in what was widely viewed as the first major attack on a nation’s power grid. About a year later, hackers seemingly used malware to capture login credentials of employees at an electricity control center. With that information, they were able to shut power to parts of Kiev—providing a taste of the potential devastation of attacks against industrial control systems.⁹
THE WAY FORWARD

Complex, ever-changing threats. Constrained budgets. Challenges in finding and retaining top security expertise. Sensitive data to safeguard. Important missions to fulfill—and innovative opportunities to use digital to deliver. How can government protect so much with resources that can never adequately address all risks and all threats? Accenture recommends a practical approach that balances cyber risks and digital rewards by embedding a rich security strategy at the core of all digital technology. Here’s how to start:

BUILD A CYBERSECURITY STRATEGY. A crisis response plan is not enough. Every government organization also needs a proactive, holistic security strategy. The strategy needs to address not only the protection and security of data and technologies, but also the integration of these with other security measures, the creation of policies “fit for purpose” in the digital age, and the training necessary for employees to be the first and last line of cyber defense.

LEAD SECURITY EFFORTS WITH INTELLIGENCE, AND RELY ON ADVANCED ANALYTICS. Digital gates and guards used to be enough to protect networks and data. No more. Effective protection now requires use of advanced threat intelligence supported by advanced, multifaceted analytics to help identify and manage threats. For instance, employee behavioral analytics use vast quantities of data from multiple sources to baseline normal network activity and identify anomalous or questionable activities in real time. Similarly, dynamic authorization management draws on behavioral and contextual data—including the sensitivity of the data being accessed and any employee risk factors—to automate in-the-moment authorization decisions.

ASSESS RISK. Conduct a risk assessment to determine the areas of greatest vulnerability and potential consequences of an attack. To engineer effective defenses, take a realistic and pragmatic view of the threat universe and most likely scenarios. Conduct the assessment with both security experts and stakeholders from throughout the agency.
INVEST IN CYBERSECURITY TALENT. Across industries, cybersecurity expertise is in short supply, and many public service organizations find themselves lacking sufficient skills and competencies to thwart the array of digital threats that both they and their citizens face. Public service leaders can respond with a hybrid approach: allocating resources to attract and build a strong in-house team, while augmenting those strengths with third-party support through in-depth partnerships with both industry and the academic community.

INCREASE STAKEHOLDER COLLABORATION. “Inside jobs”—that is, data theft, leakage or corruption by employees, whether intentionally or not—are among the most common sources of cybersecurity breaches. Thus, it is crucial to educate employees so everyone can play their part in protecting data. In particular, government employees need to understand the risks and security protocols when using mobile devices, leveraging their social media and other on-line tools to demonstrate their digital prominence, or accessing systems and data in the cloud. Alongside employee awareness and training, government needs to work with peer organizations, academia and the private sector to minimize risk. Such partnerships aren’t just about filling roles – they also aim to ensure that government agencies are receiving innovative, ever-evolving thinking into security solutions today through refreshed thinking, insights and skills drawn-in from outside government.

While every industry is facing challenges around keeping systems and data safe, government agencies face additional layers of risk and complexity. Securing public services and information requires a state-of-the-art mindset: one that evolves and adapts based on changing conditions and threats, and that incorporates a distinct blend of government, technology and security expertise. In so doing, government organizations will be best-placed to address both the evolving cyber-threat landscape and take maximum advantage of today’s evolving technologies to support their citizen services in the most safe, secure manner possible.
EXPERTS:

Dr. Kevin A. O’Brien
Senior Principal, Global Security & Intelligence
Health & Public Service, Accenture
kevin.obrien@accenture.com
@kaobrien15
https://www.linkedin.com/in/kaobrien70/

Dr. Valtteri Vuorisalo
Senior Principal, Global Defense & Security
Health & Public Service, Accenture
valtteri.vuorisalo@accenture.com
@vvuorisalo
https://www.linkedin.com/in/vvuorisalo/

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

NOTES

3. Business Insider
4. Reuters