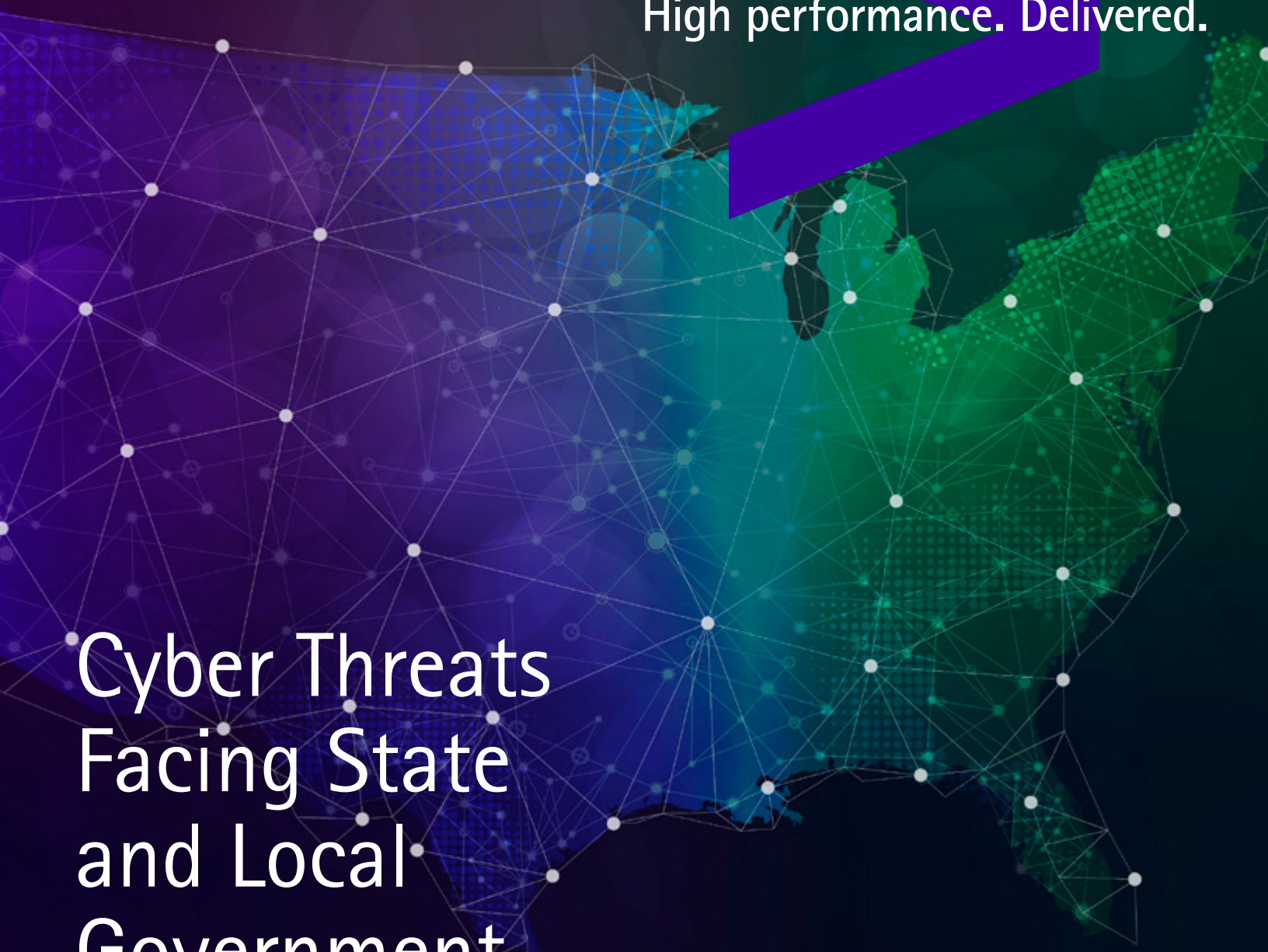
accenture consulting

High performance. Delivered.



Cyber Threats Facing State and Local Government

Strategy | Consulting | Digital | Technology | Operations

As cyber threats increase in number and sophistication, organizations across industries are seeking more effective ways to protect themselves: their data, their infrastructure, their people and their reputations. State and local governments are no exception.

For the past five years, CIOs have ranked security and risk management as a top concern for state governments. It's been their number-one concern for the past three years—with good reason.[1] State and local governments may be especially vulnerable to cyber attacks and other security breaches. According to the Security Scorecard 2016 Cybersecurity Report, "[w]hen compared to the cybersecurity performance of 17 other major industries, government organizations ranked at the bottom of all major performers, coming in below information services, financial services, transportation and healthcare."[2]

Further, the State of Software Security, Volume 6, Focus on Industry Vertical, cites government's low rate of compliance with OWASP[3] Top 10 Policy on First Risk Assessment. In government, the pass rate was just 24 percent, twice as low as the pass rate in financial services. In addition, government had the highest prevalence of vulnerability in code quality—along with the highest prevalence of both SQL Injection and Cross-Site Scripting on first assessment.[4]

The U.S. government was hit by more than 77,000 "cyber incidents"—including data thefts and other security breaches—in fiscal year 2015. While only a relatively small number of those incidents would be considered significant breaches, a White House audit revealed that the total number of incidents represents a 10-percent increase over the previous year.[5]

Why has government become such a desirable target? First, cyber criminals are eyeing the citizen data and other sensitive information that governments manage. Personal data—from Social Security numbers and driver's license records to health and tax information—can be valuable on the black market. Second, as governments work to digitize services, many are doing so with an aging infrastructure and funding constraints. Among the other factors compounding the risks: government's aging workforce and challenges around identifying, recruiting and retaining security skills, which are increasingly in demand by virtually every sector. Finally, under-investment in IT consolidation and security initiatives has left state and local governments vulnerable.

In the news: Security breaches

For evidence of the risks, consider just a few examples of reported breaches and incidents in recent years.

June 2016: A security researcher discovers that an unnamed client of L2—a U.S.-based company that builds, manages and sells access to voter records—has been breached. Hackers took down the firewall for the client's database hosted on a Google cloud server. The database contained Personally Identifiable Information (PII) belonging to 154 million U.S. voters, representing 62 percent of all voters.[6]

June 2016: A hacker using the name of NSA takes to the Dark Web, offering for sale a dataset containing personal details and driver's license information of more than 290,000 U.S. citizens. The hacker discloses that he obtained the data after breaching the networks of several Louisiana organizations.[7]

June 2015: Leaked U.S. government log-in credentials—including data belonging to 705 government staff from 47 U.S. government agencies—are reportedly found on public paste sites. Although it is unclear how many of the credentials were active or how many passwords were current, the credentials were most likely stolen via malware-infected websites.[8]

May 2015: Hacktivists operating as Anonymous target the Baltimore Police Department following the death of Freddie Gray. Announcing their support for those protesting the police, Anonymous discloses some information belonging to the department—including multiple email addresses and IP addresses for some Internet services used by the authorities.[9]

October 2014: The City of Phoenix's network goes down for nearly an hour on October 25 thanks to a hacker-initiated denial of service (DoS) attack. The DoS attack blocks access to the city's website and online services while also disrupting the police department's computers.[10]

October 2014: The Oregon Employment Department (OED) notifies more than 850,000 individuals registered with WorkSource Oregon Management Information System that their information—including Social Security numbers—might have been compromised.[11]

Meeting the challenges

In the face of mounting security threats and risks, state and local organizations need to balance meeting their missions and protecting their enterprises. That requires attention to a number of key areas: defending against cyber-attacks; automating threat intelligence, remediating vulnerabilities and responding to incidents; managing digital identities across many platforms and channels; attracting top security talent; and supporting cloud enablement.

Accenture offers a suite of services to help state and local governments tackle those priorities. Our approach to security offers state and local government organizations end-to-end transformational services:

Assess & Architect – Threat & Vulnerability Assessment & Remediation, Application Security Assessment & Remediation, Discovery & Protection of High Value/Data Assets, Capability Maturity & Technology Assessment, Enterprise Security Architecture and Security Compliance Assessment

Cyber Defense – Threat Intelligence, Vulnerability Management, Operational Monitoring, Advanced Security Analytics and Security Incident Management

Digital Identity – Enterprise Identity & Access Management, Customer Identity & Access Management, Identity of Things and Next Generation Authentication

Emerging Technology Security – Cloud Security, Mobile Security, Industrial/Operations Internet of Things (IOT) and Consumer/Device IOT

Managed Security – Managed Cyber Defense, Managed Identity and Managed Compliance

For more information, please contact:

Keir Buckhurst
Managing Director,
Technology Consulting
keir.buckhurst@accenture.com

Lalit Kumar Ahluwalia
North America Security Lead—
Public Sector/Higher Ed
lalit.k.ahluwalia@accenture.com

Connect with us to learn more on Twitter: @AccenturePubSvc

Or visit: www.accenture.com/publicservice

References

[1] Source: NASCIO, Survey of State CIO Priorities for 2016. http://www.nascio.org/Portals/0/Publications/Documents/2015/State_CIO_Top%20_Ten_Policy_and_Technology_Priorities_for_2016.pdf

[2] Source: Security Scorecard, 2016 Cybersecurity report.

[3] OWASP stands for Open Web Application Security Project.

[4] https://www.veracode.com/sites/default/files/Resources/Reports/state-software-security-report-june-2015-report.pdf?mkt_tok=eyJpIjoiTkdSaE0yWTFZMlEwTVRrMSIsInQiOiI0ck5QekFkMmlTQ0hjaINSaGtMOTFzam40RHRKeXB2MVFxZzVQQ0pJdE9FQ1NHbFwvTVJjMTFyRTk1ODRjY0NKc21KZjhndFc4eUliZ2tsZWErTE9WQXBsdlNQN2Nc21KZjhndFc4eUliZ2tsZWErTE9WQXBsdlNQN2Nlb1BMQVVmQkE4R2p1NGM9In0%3D

[5] Source: Number of US Government Cyber Incidents jumps in 2015. March 2016. https://www.yahoo.com/news/number-u-government-cyber-incidents-jumps-2015-205016646.html?ref=gs

[6] http://news.softpedia.com/news/hackers-breach-us-company-and-unwittingly-expose-154-million-voter-records-505553.shtml

[7] http://news.softpedia.com/news/hacker-puts-up-for-sale-290-000-us-driver-s-license-records-505161.shtml

[8] http://www.scmagazine.com/analysis-of-17-paste-sits-uncovers-login-credentials-from-47-govt-agencies/article/422921

[9] http://news.softpedia.com/news/Hackers-Leak-Baltimore-Police-Data-480036.shtml

[10] http://www.fox10phoenix.com/story/27055272/2014/10/28/city-of-phoenix-under-attack-by-hacker-activists

[11] http://www.kptv.com/story/26776035/worksource-oregon-data-breach-affects-850000-people

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 more than 375,000 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.

Accenture Information Security Team

Accenture brings important expertise to address these complications and other cyber security issues. Accenture's global security team has several offerings focused on assessing and responding to cyber threats, including Active Defense and Threat & Vulnerability Management. In August 2015, Accenture also acquired FusionX, a U.S.-based cyber security company that offers cyber attack simulation, threat modeling, cyber investigations and security risk advisory services. FusionX's expertise in identifying security vulnerabilities and Accenture's industrialized suite of security transformation and operations offerings enable companies to more effectively manage risk and improve business results.

Accenture Materials

Security Services–Accenture.com

Accenture News–Acquisition of FusionX

Accenture's Security Services

From security strategy to transformation to managed security services, Accenture's 360-degree approach helps organizations tackle the entire spectrum of security challenges, taking into account people, processes and technology. Serving as a trusted security partner to more than 330 corporations and governments across the globe for more than 20 years, Accenture's Security Services include advanced solutions that detect, respond to and remediate security breaches, as well as pre-empt and prevent future attacks. By providing intelligent security services designed to outpace sophisticated attackers, Accenture helps its clients become resilient so they can turn their focus to what matters most: innovation and business growth, uninterrupted. More information:

Security that sets you free

Fewer threats. More time to innovate.

Technology Vision 2016: Digital Trust