BCG

The Boston Consulting Group

Cybersecurity in a Fractured World

THE CYBERSECURITY ASSISTANCE LOCAL GOVERNMENTS NEED

By David Mkrtchian, Andrew Smolenski, Stefan Deutscher, Troy Thomas, and Walter Bohmayr

This is the first in a series of articles and interviews on the subject of improving cyberresilience—the ability of companies, organizations, and institutions to prepare for, respond to, and recover from cyberattacks. Other articles in the series, which is a product of BCG's work with the World Economic Forum, will examine such topics as the security requirements of critical IT infrastructure, how boards of directors and senior managers should approach cybergovernance, and how businesses undergoing digital transformation can ensure that cybersecurity is considered deliberately rather than on an ad hoc basis.

The former chairman of the US National Governors Association, Terry McAuliffe, made cybersecurity at the state and local levels the focal point of his tenure. With good reason. US public-sector entities rank third for data breaches, behind only financial institutions and health care organizations, according to Verizon's *2017 Data Breach Investigations Report.* If yet another warning was needed on the dangers of poor or inadequate cybersecurity, it came in the form of the hacking of the Equifax credit rating agency, which exposed more than 140 million US consumers to identity theft from May to July of 2017.

Many experts have long pointed to state and local governments as a weak link in cybersecurity, because they lack the sophisticated defenses and incident response systems employed by the federal government and national defense agencies. The vulnerability is especially serious since it often involves "critical infrastructure"—bridges, tunnels, highways, and hospitals, for example. Moreover, vulnerable local-government systems can provide a beachhead for those looking to infiltrate state or federal networks.

A Big Local Need…

Here's the rub. State and local governments are typically poorly suited to addressing cybersecurity on their own. Not only do they lack funding for the latest solutions, they do not have the scale, skills, or expertise to assess the risks and vulnera-

bilities that they face or the solutions that can help them develop better cyberresilience.

It's worth pausing to reflect on the technology landscape. BCG's analysis of global cybersecurity startup activity identified about 1,000 firms in 14 clusters, including data security, network security, mobile device security, disaster recovery, and identity theft and authentication, with a total of some $20 billion of investment behind them. (See the exhibit.) The cloud continues to put more security solutions within reach, while at the same time introducing new concerns about its own security. And technological progress and innovation in everything from artificial intelligence to behavioral analytics increase the number and complexity of products and services.

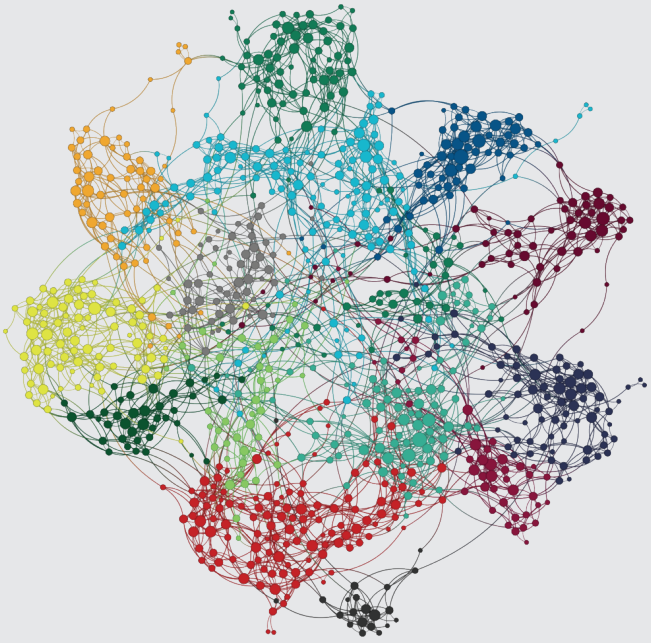
Citizens rightly expect government to take steps to protect against cyberattacks. But it is unreasonable to expect state and local governments to navigate the global hive of cybersecurity activity on their own and to implement solutions to protect themselves and the digital assets of their constituents.

Yet this is exactly the path that public-sector cybersecurity is on. And right now, apart from the laudable general recommendations developed by the National Institute of Standards and Technology, pretty much the only source of advice for state and local purchasers of security software and solutions are the market research and advisory firms that assess new products and solutions. While these firms strive to be helpful and objective, they are often compensated by the companies offering the products in question—a situation not unlike that of the credit rating agencies that were paid by issuers to assess debt offerings prior to the 2008 financial crisis.

…Can Benefit from Federal Help

Washington can help—without imposing a "federal solution." Indeed, many local governments are already looking upward for support. Money is one issue, but there are other useful forms of assistance. One could be shared services: the federal government makes the cybersolutions that it uses available to local governments on a voluntary

More Than 1,000 Startups Compete in a Fragmented Cybersecurity Market



CYBERSECURITY CLUSTERS	Startups (%)	Funding (%)
Mobile device security	13	16
Penetration testing & incident response	13	6
Cloud security	10	10
Data security & solutions	9	13
Endpoint security	8	10
Disaster recovery & secure hosting	8	6
Email security	6	8
Identity & access management solutions	6	7
Network security	6	8
Identify theft & authentication	6	3
Web application security	5	2
Secure enterprise communication	4	4
Security analytics	4	5
Managed security services	2	2

Sources: Quid; BCG Center for Innovation Analytics; BCG analysis.
Note:. About 1,000 companies (startups only) involved in the cybersecurity industry were clustered using Quid software based on similar products, technology, customers, and other criteria. The Quid database includes companies that have received equity investment since 2011.

basis. Another valuable form of assistance may be expertise: enabling state and local entities to make informed decisions about their cybersecurity needs and the potential solutions. Experts typically divide cybersecurity into three components: people, processes, and technology. By lending its expertise and experience in technology, the federal government can help local governments set priorities and develop strategies and plans—and implement them—while local governments maintain authority and control over their own systems. In France, for example, the national cybersecurity agency (ANSSI) provides several cybersecurity services for government agencies at all levels, including an accreditation process for security solutions. And Germany is establishing a central office for IT that can provide services to security agencies.

Federal assistance can take several forms.

Sharing Expertise and Solutions. The federal government can supplement state efforts (such as recent ones led by the National Governors Association) with information that helps local governments assess their needs. What kind of end-to-end coverage do states (or municipalities) require? Does a state or city need both a secure web gateway and a firewall? How do states and cities connect with federal systems in a secure manner? What industrial control systems are particularly vulnerable (a topic of particular salience for public utilities)? In short, which features are relevant? And after the necessary features have been determined, what are the right questions to ask vendors about the customization and integration of solutions? How should contracts be structured to ensure that vendor compensation is aligned with the goal of improved security?

Building a Clearinghouse. The federal government can provide a clearinghouse function for cybersecurity products, services, and solutions (making use of existing evaluations done by the defense agencies). Think about a central resource where companies submit their services and solutions for formal certification or approval. (The Common Criteria for Information Technology Security Evaluation, an international computer security standard, can provide a helpful blueprint.) Companies would be keen to get their services on the list, since approval would lead to sales, and local governments would know that any approved service on the list has been assessed by experts.

Taking Advantage of Buying Power. By extending the clearinghouse concept to a marketplace, the federal government could marshal its buying power on behalf of state and local purchasers, bringing prices down without having to purchase a thing itself. Vendors would stand to benefit from such a centralized marketplace. By not having to pitch to thousands of subnational entities individually, they could save on nonimplementation sales costs and reinvest those funds in developing additional security features. There might be initial resistance from firms that do make the approved list, but those companies could also be encouraged to upgrade their offerings to meet federal standards.

Startups with innovative solutions would be on a level playing field with large security companies. The size of a company's marketing budget would be less important than its underlying technology, solutions, and ability to serve a customer's needs. Existing security companies could benefit from the existence of a neutral arbiter that separates the wheat from the chaff and ensures that vaporware does not overtake trusted solutions. In the end, state and local governments would be assured of getting quality solutions at a price negotiated by experts backed with buying power. The federal government would help make the cutting edge of cybersecurity more accessible not only for well-funded enterprises but for governments—and the citizens they serve—at all levels.

We live in a connected world. Recent attacks have shown how fast that connectivity can be turned against us. Strengthening cyberdefenses requires a coordinated response. Everyone suffers if local governments are left vulnerable.

About the Authors

David Mkrtchian is a consultant in the New York office of The Boston Consulting Group. You may contact him by email at mkrtchian.david@bcg.com.

Andrew Smolenski is a project leader in the firm's San Francisco office. You may contact him by email at smolenski.andrew@bcg.com

Stefan Deutscher is an associate director in BCG's Berlin office. You may contact him by email at deutscher.stefan@bacg.com.

Troy Thomas is an associate director in the firm's Washington, DC, office. You may contact him by email at thomas.troy@bcg.com.

Walter Bohmayr is a senior partner and managing director in BCG's Vienna office. You may contact him by email at bohmayr.walter@bcg.com.

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with more than 90 offices in 50 countries. For more information, please visit bcg.com.