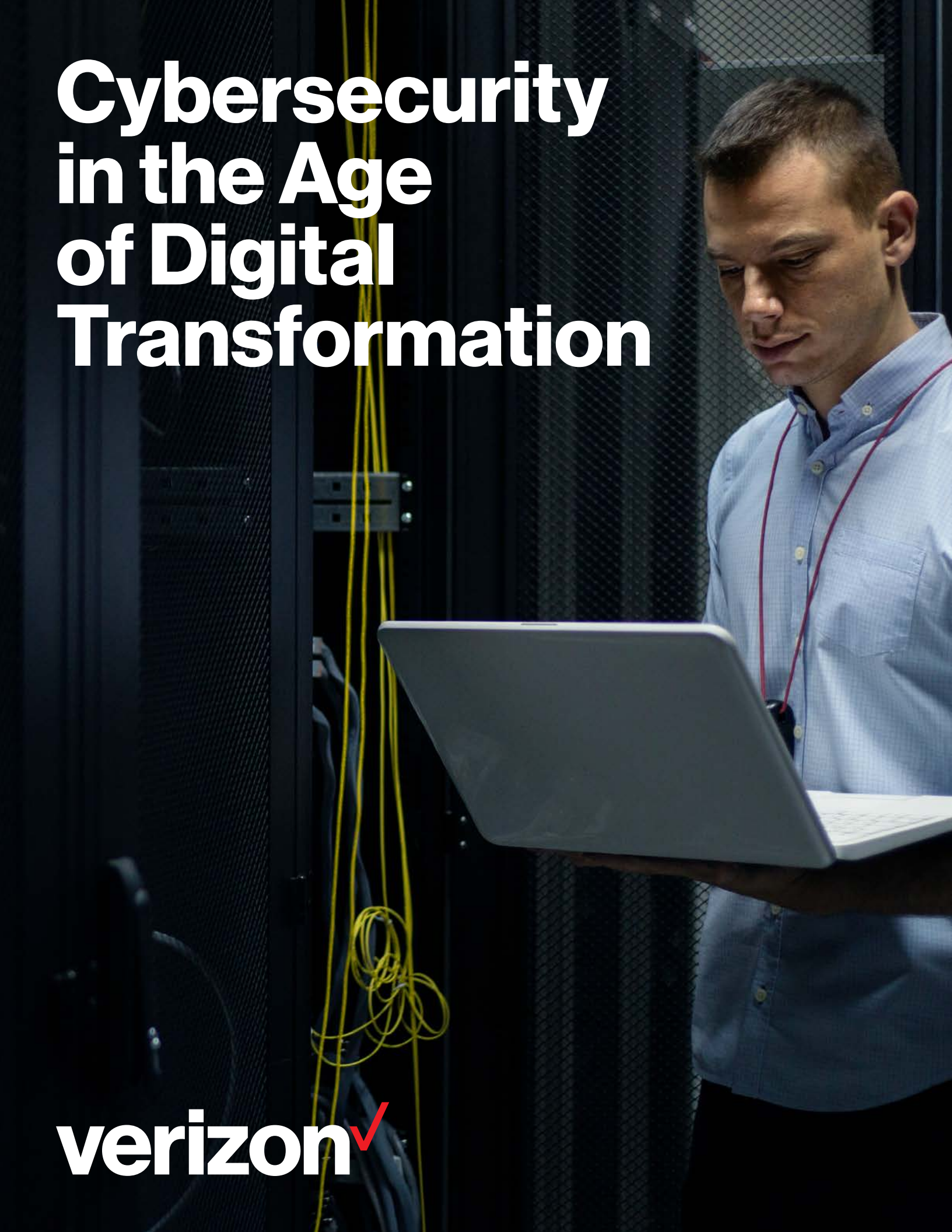
# Cybersecurity in the Age of Digital Transformation



verizon

As government agencies seek to enhance mission outcomes and improve citizen services through IT modernization and digital transformation, security considerations must remain at the forefront.

This paper outlines the cybersecurity challenges facing government organizations today, and provides concrete steps toward improving security.

## Challenges Persist

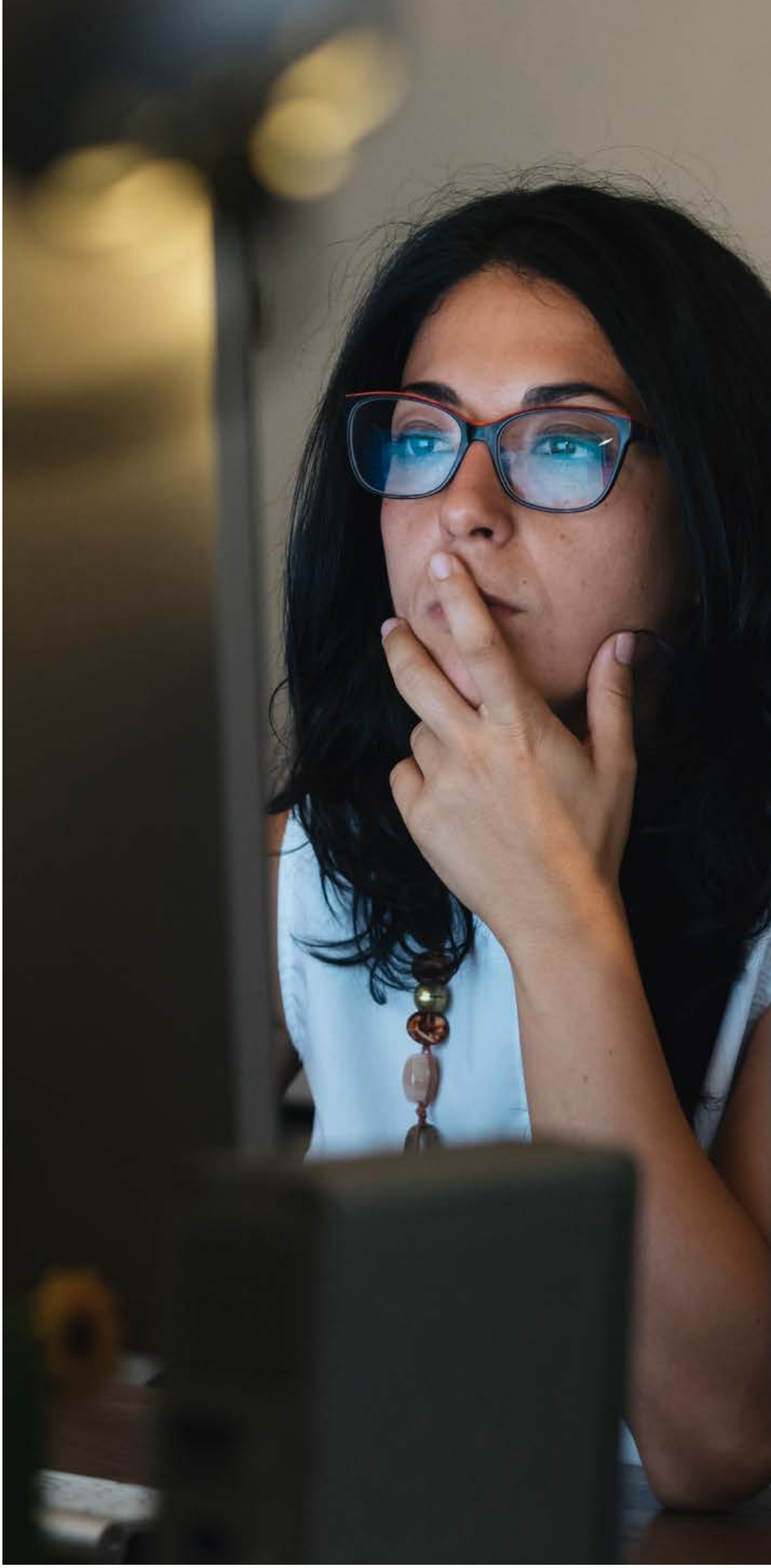
Cybersecurity is a continuing challenge for all organizations, no matter the sector or size. There were more than 41,686 incidents and 2,013 confirmed data breaches in 2018, according to Verizon's 2019 Data Breach Investigations Report: Public Sector (DBIR). The DBIR study found that the public sector faces a specific and rapidly growing set of cybersecurity challenges. For example, breaches caused by cyber-espionage attacks against government agencies grew 182% in 2018 year-over-year from 2017. 75% of these attacks came from external actors, the vast majority of which were state-affiliated. In looking at how these attacks were made, phishing was the top tactic.

The DBIR study found that government agencies face a specific set of cybersecurity challenges. For example, the public sector is a top target in social breaches, including phishing and pretexting attacks, reporting 96 such incidents in 2017 compared with 56 in the healthcare industry, 41 in education, and 25 in the financial services sector.

Phishing is the crafting of a message that is sent typically via email and is designed to influence the recipient to "take the bait" via a simple mouse click. That bait is most often a malicious attachment but can also be a link to a page that will request credentials or drop malware. Pretexting is the creation of a false narrative to obtain information or influence behavior.

Overall, it's not entirely surprising to see the prevalence of cybersecurity incidents in the public sector. David Hylender, a Verizon senior risk analyst and DBIR report co-author, recently told GovTech magazine: "The government is kind of [between] Scylla and Charybdis in that they are both one of the country's largest employers and have tons of information about the public at large, and they store a great deal of sensitive strategic and military data."

In addition, complex departmental hierarchies and disparate or outdated IT infrastructure can make it difficult to enforce consistent security policies. That's perhaps why government organizations were the second-most likely to say that they have suffered downtime or data loss, according to Verizon's 2019 Mobile Security Index.



## Advice and Strategy

Despite the challenges before them, there are practical, effective steps that government agencies can take. Preventative and proactive measures, including training and technology, can help better protect and secure people, processes, and assets.

**1. Understand the threats**
Governments have a unique relationship to the people whose data they maintain. They are storing information not only for the citizens they serve, but also the individuals under their employ, and remain the largest employer for most countries.

**External threats:** Agencies must recognize that personal information is a prime target among cybersecurity incidents. As they digitally transform and modernize IT systems, it's critical to take account of security policies and the need to protect sensitive information. A part of that includes proper access management and policy control. Access privileges should be provided on a "need to know" basis, and there should be programs in place to ensure access to systems is closed when employees leave the organization.

**Internal threats:** In addition, insider threats are a significant cybersecurity concern. Most issues tend to be password-related or accidental versus malicious behavior. For example, users may unknowingly click a link that downloads malware, or create weak passwords for access to systems with sensitive data.

**2. Take action:**
Digital transformation is underway, with government agencies now collecting, storing, and processing more data. That's why now is the time to ensure there is a comprehensive security plan in place to secure and protect that data — rather than bolting on a solution after the fact.

There are straightforward actions government agencies can take to strengthen security while digitally transforming (see Action Checklist box). The key is to take a holistic view of systems, processes, and users.

### At a minimum, follow this Action Checklist:

- **Don't wait to find out about a breach from law enforcement.** Deploy log files and change management systems that offer early warning of a security compromise.
- **Conduct ongoing employee training.** Teach users how to spot the signs of an attack and how to react.
- **Limit access to the people who need it** to do their jobs, and have processes in place to revoke it when they change roles.
- **Conduct routine monitoring and security audits.**
- **Patch promptly and keep anti-virus software up to date.**
- **Encrypt sensitive data** to render it useless if it is stolen.
- **Use two-factor authentication** to limit the damage that can be done if credentials are lost or stolen.
- **Use physical security systems.** Surveillance cameras and entry systems for restricted areas, for example, can help mitigate the risk of criminals tampering with systems or stealing sensitive material.

**3. Prioritize adoption of technologies designed with security in mind**
Agencies should look to adopt technologies with proven successes in the commercial sector, and tailor them to their needs. Now is the ideal time to combine IT modernization efforts with technology that protects data, systems, and people, while still supporting specific public sector requirements. In the U.S., these include cloud security programs like Federal Risk and Authorization Management Program (FedRAMP), and the requirement to maintain U.S. federal data within the United States.

**Virtualization:** Unlike legacy systems that are often unencrypted, the implementation of virtualized services streamlines encryption and makes data access controls easier to manage. In addition, virtualized networks are better able to handle distributed data, while also maintaining security and improving flexibility capabilities compared with legacy systems. For example, the use of software defined perimeter (SDP) allows approved users to access network resources. It authenticates identities and devices, "hiding" enterprise apps and resources from attackers.

**Reduced attack surface:** Multiple disparate pieces of hardware increase cybersecurity risks. Moving to the cloud or a virtualized network enables agencies to shrink and better manage the attack surface.

**Software-defined approaches:** Software-defined perimeter, networking (SDN) and wide-area network (SD-WAN) solutions not only help control physical assets and capital expenditures with less hardware to buy, but they also simplify and speed the ability to deploy, change or take down services, bringing massive scalability and flexibility.

An SDP platform provides strong validation when users access network resources. It authenticates identities and devices, including locations and certificates. This managed service helps agencies avoid the risk of potential attacks at the virtual border, securing both users and the IT infrastructure.

SDN and SD-WAN solutions can also address security concerns. For example, mobile, cloud, video, VoIP, presence and Internet of Things are driving increasing bandwidth requirements. On the flip side, these applications are spotlighting the need for higher quality of service (QoS) and strong security. They pose particular challenges to the traditional WAN connecting mobile users and branch offices to headquarters.

SD-WAN technology is better able to handle the load with high QoS and security while managing costs. It enables the agency to route mission-critical traffic — such as applications considered essential for customer interaction as well as workforce productivity — on a policy-defined, app-by-app basis through high-quality, private WAN connections, while offloading non-critical traffic to internet and broadband connections. It uses the SDN architecture, which separates the control plane from the data plane, to dynamically assign bandwidth and other resources as demand changes.

In a nutshell: These solutions provide agencies with flexible connectivity in a single, unified, highly secure network.

## Summary

As they seek to modernize and digitally transform, the time is now for government agencies to address cybersecurity issues with a comprehensive strategy. That must take a holistic view to:

- Understand the external and internal threats
- Create a holistic security strategy, but prioritize a few critical actions right away
- Prioritize adoption of technologies designed with security in mind

These strategies are significantly enhanced when agencies leverage services from experienced, reliable vendors. Technology partners will work hand-in-hand with IT departments to securely run network operations, assist in employee training efforts, and improve the organization's overall cybersecurity posture.

### Into the Data Breach

Verizon analyzed 330 public sector data breaches in 2018, the highest number among all industries, according to the 2019 Data Breach Investigations Report: Public Sector. Among the top causes for these breaches were:

- Cyber-espionage (42%)
- Miscellaneous errors (18%)
- Privilege misuse (12%)
- Everything else (11%)
- Web applications (10%)