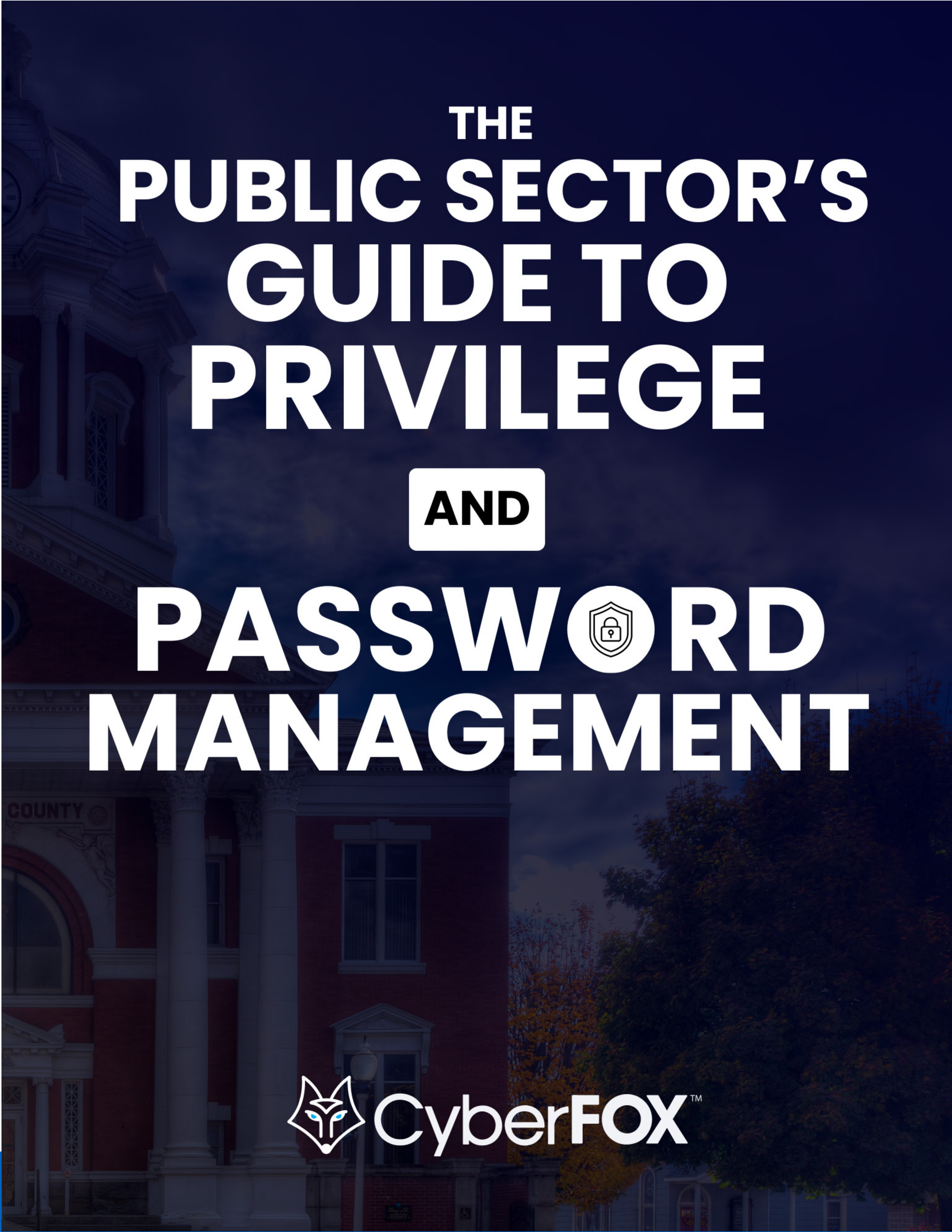
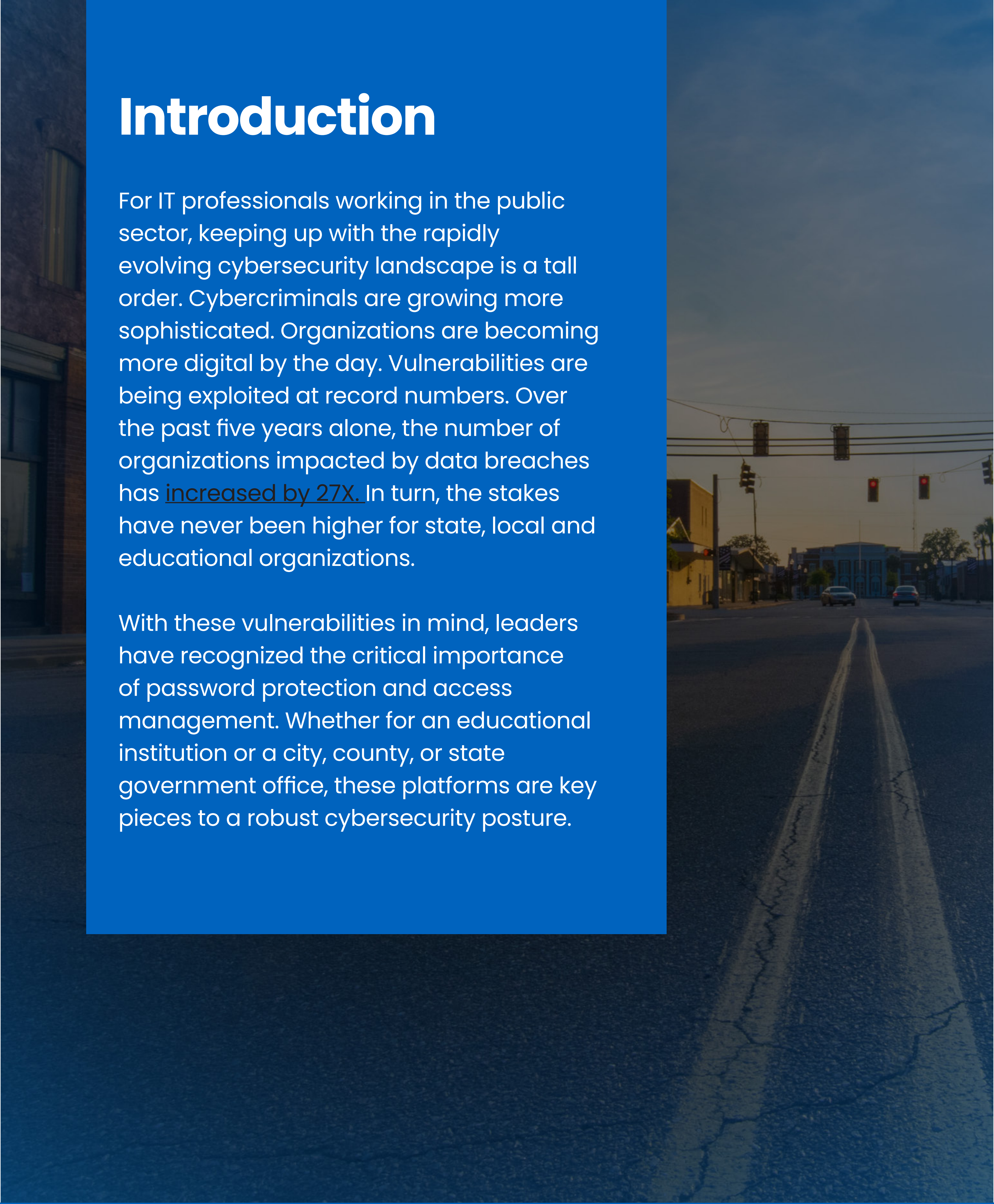


THE PUBLIC SECTOR'S GUIDE TO PRIVILEGE AND PASSWORD MANAGEMENT

CyberFOX™

Table of Contents



Introduction

For IT professionals working in the public sector, keeping up with the rapidly evolving cybersecurity landscape is a tall order. Cybercriminals are growing more sophisticated. Organizations are becoming more digital by the day. Vulnerabilities are being exploited at record numbers. Over the past five years alone, the number of organizations impacted by data breaches has increased by 27X. In turn, the stakes have never been higher for state, local and educational organizations.

With these vulnerabilities in mind, leaders have recognized the critical importance of password protection and access management. Whether for an educational institution or a city, county, or state government office, these platforms are key pieces to a robust cybersecurity posture.

Chapter 1

Why are Public Institutions a Target?

Cyberattacks targeting government agencies are on the rise. In 2023, 78% of education and government entities reported cybersecurity staffing shortages. Coupled with the factors below, these shortages have turned school districts, elected offices, and municipal departments into prime targets.

While many cybercriminals are driven by financial gain, others are prompted by more intrinsic motivations such as fanaticism or political ideologies. Here's a look at public entities from the perspective of a cybercriminal:

1. Abundant sensitive data to sell on the dark web, including social security numbers, personal addresses, and financial records.
2. Weak cybersecurity measures due to limited budgets, outdated software, plentiful access points, and staffing shortages.
3. High disruption potential for essential services such as public safety, thereby increasing the likelihood of ransom payments.

Chapter 2

The Impact of a Cyberattack

Today, the average cost of a data breach has soared to nearly $4.5 million. At the same time, not all costs are quantifiable. In the aftermath of a cyberattack, leaders are often faced with a myriad of financial and non-financial challenges, such as:

- Legal fees and settlements resulting from damages
- Fines imposed by regulatory bodies
- Outreach costs to notify the victims
- Operational downtime and service disruptions
- Reputation damage
- Higher insurance premiums
- Third-party breach response services
- And increased cybersecurity measures

Unfortunately, cybersecurity is often an afterthought in the wake of a cyberattack. By investing in preventative Privilege Access Management and password management solutions, leaders can mitigate these costly risks.

Chapter 3

Common Cybersecurity Oversights

Given the 74% YoY increase in ransomware attacks, good cyber hygiene has never been more important. From simple practices like frequent password changes to more advanced measures like end-to-end encryption, taking preventative action today is key to thwarting cyberattacks. The question is, which actions should be taken? Here are a few common oversights that having a Privilege Access Management and Password Management solutions can addresses:

1. **Excessive admin access** to nonessential personnel.
2. **Simple passwords** that can be easily guessed.
3. **Inadequate encryption** for sensitive information.
4. **Lack of 2FA** to prevent illegitimate login attempts.
5. **Over-reliance on manual tasks** among cybersecurity personnel.
6. **Cumbersome audit logs** that can't be searched easily.
7. **Antiquated devices** that can't be wiped remotely.

Even a well-informed staff can make honest mistakes that leave organizations vulnerable, such as losing a laptop or clicking a legitimate looking email attachment or link that is actually connected to a phishing scheme.

The right cybersecurity platforms should account for human error.

Fortunately, each of the oversights above can be addressed by effective Privilege Access Management (PAM) and password management solutions.

Chapter 4

What Is Privileged Access Management (PAM)?

For educational institutions and government offices, different users should have different access levels despite sharing the same system. For example, a student shouldn't be able to see the same data and access the same controls as the school's principal. As a result, having an effective privilege access management solution is key. Whether that's removing local admin rights by department, automating rules and office policies, or managing privileges, PAM solution like AutoElevate reduce risks by making least privilege access actionable.

Chapter 5

What Is Password Management?

Today's desk workers regularly use an average of 11 applications and digital platforms. In turn, the temptation to use simple passwords is high, leaving their parent organizations at risk. That's where a user-friendly password management platform like Password Boss can help. How? By introducing end-to-end encryption, 2FA, and auto-logins for authorized users. The result is a more secure organizations and a less frustrated workforce.

Chapter 6

When Vulnerabilities are Exploited

The rising threat of cyberattacks is best demonstrated through real-world situations. An attack in late 2023 on a Pittsburgh-area water system is a stark reminder of what is at stake. Here, the Municipal Water Authority of Aliquippa fell victim to hackers who disabled critical automated control systems. The group responsible for the attack, CyberAvengers, was said to have gained access by exploiting a weak password that could have been protected using 2FA.

Here, a small township was affected by the attack, prompting an immediate investigation from the U.S. Department of Homeland Security. This is a wake-up call for government agencies leaders who may think their organizations aren't a target. The truth is that no government organization or school district is too small to be targeted.

Chapter 7

AutoElevate by CyberFOX

As an affordable Privilege Access Management (PAM) platform for public organizations, AutoElevate makes least privilege access simple and enforceable at scale. Here's how:

- **As-needed privileges** to specific apps and actions.
- **Automated rules** that align with your district or office policies.
- **Privilege management** from anywhere using remote access.
- **Request management** in real-time from a unified dashboard.
- **Simple audit logs** that flag risky behavior.
- **Blocklisting** to thwart malicious attacks.

Chapter 8

Password Boss by CyberFOX

From encryption using 2048-bit RSA key pairs to role-based access, Password Boss has dozens of protective features without sacrificing productivity. Here's what's included:

- **Automatic data wiping** for lost or stolen devices.
- **Limited access** for users based on their needs.
- **End-to-end encryption** to protect passwords.
- **Auto-logins** across devices for authorized users.
- **Seamless integrations** with IT tools.

Password Boss and AutoElevate align with all Family Educational Rights and Privacy Act (FERPA) and HIPAA standards for educational institutions while complying with state and local regulations for government offices.

Chapter 9

Mitigating Tomorrow's Risks

By 2027, the cost of cybercrime on the global stage is poised to reach $23 trillion. Along the way, state and local government offices, educational institutions, and other public sector entities will remain a prime target for syndicates. As a result, the importance of preventative protection has never been greater.

Public sector leaders have a responsibility not only to their staff, but also to constituents, parents, and the community as a whole.

Given that two-thirds of US consumers say they would not trust a company with their data after a breach, the importance of proactive protection is clear.

Ultimately, the best way to remediate the reputation damage and distrust of a cyberattack **is to avoid the cyberattack in the first place.**

Chapter 10

Getting Started with CyberFOX

CyberFOX empowers both educational institutions and government offices to mitigate the risk of a cyberattack. By integrating seamlessly with the platforms you're already using, AutoElevate and Password Boss improve your security posture without disrupting your day-to-day workflows.

Don't let your organization make the headlines for a cyberattack. The time is now to fortify your defenses with CyberFOX. If you still have questions, we invite you to reach out to us today. You can also access a free trial for both AutoElevate and Password Boss to get a hands-on feel for heightened protection.