Harvard Business Review

POLICY

8 Ways Governments Can Improve Their Cybersecurity

by Michael Chertoff and Jeremy Grant

APRIL 25, 2017

It's hard to find a major cyberattack over the last five years where identity — generally a compromised password — did not provide the vector of attack.

Target, Sony Pictures, the Democratic National Committee (DNC) and the U.S. Office of Personnel Management (OPM) each were breached because they relied on passwords alone for authentication. We are in an era where there is no such thing as a "secure" password; even the most complex

password is still a “shared secret” that the application and the user both need to know, and store on servers, for authentication. This makes passwords inherently vulnerable to a myriad of attack methods, including phishing, brute force attacks and malware.

The increasing use of phishing by cybercriminals to trick users into divulging their password credentials is the most alarming — a recent report from the Anti-Phishing Working Group (APWG) found that 2016 was the worst year in history for phishing scams, with the number of attacks increasing 65% over 2015. Phishing was behind the DNC hack, as well as a breach of government email accounts in Norway, and was the method that state-sponsored hackers recently used in an attempt to steal the passwords of prominent U.S. journalists. Phishing is on the rise for a simple reason: it is a relatively cheap and effective form of attack, and one that puts the security onus on the end-user. And, given that many users tend to reuse passwords, once these passwords are compromised, they can be used to break into other systems and bypass traditional network security measures.

In response to the increased frequency of such authentication-based cyberattacks, governments around the world are pursuing policies focused on driving the adoption of multi-factor authentication (MFA) solutions that can prevent password-based attacks and better protect critical data and systems. The U.S., UK, EU, Hong Kong, Taiwan, Estonia and Australia are among the countries that have focused on this issue over the last five years.

One challenge countries face: there are hundreds of MFA technologies vying for attention, but not all are created equal. Some have security vulnerabilities that leave them susceptible to phishing, such as one-time passwords (OTPs) — a password that is valid for only one login session or transaction — which, while more secure than single factor authentication, are themselves still shared secrets that can be compromised. Some solutions are unnecessarily difficult to use, or have been designed in a manner that creates new privacy concerns.

As policymakers work to address these authentication issues, they will need to adopt solutions that move away from the shared secret model while also being easy for consumers and employee to use. Per a new white paper that The Chertoff Group published, governments can best ensure the protection of critical assets in cyberspace by following eight key principles for authentication policy:

1. **Have a plan that explicitly addresses authentication.** While a sound approach to authentication is just one element of a proper approach to cyber risk management, any cyber initiative that does not include a focus on strong authentication is woefully incomplete.

2. **Recognize the security limitations of shared secrets**. Policymakers should understand the limitations of first-generation MFA technologies such as OTPs that rely on shared secrets and look to incent adoption of more secure alternatives, such as those that utilize public key cryptography where keys are always stored on — and never leave — the user's device, like FIDO authentication standards.

3. **Ensure authentication solutions support mobile**. As mobile transaction usage grows, any policy that is not geared toward optimizing use of MFA in the mobile environment will fail to adequately protect transactions conducted in that environment.

4. **Don't prescribe any single technology or solution — focus on standards and outcomes**. Authentication is in the midst of a wave of innovation, and new, better technologies will continue to emerge. For this reason, governments should focus on a principles-based approach to authentication policy that does not preclude the use of new technologies.

5. **Encourage widespread adoption by choosing authentication solutions that are easy to use**. Poor usability frustrates users and prevents widespread adoption. Next-generation MFA solutions dramatically reduce this "user friction" while offering even greater security gains. Policymakers should look for incentives to encourage use of next-generation MFA that addresses both security and user experience.

6. **Understand that the old barriers to strong authentication no longer apply**. One of the greatest obstacles to MFA adoption has been cost — previously, few organizations could afford to implement first-generation MFA technologies. Today, there are dozens of companies delivering next-generation authentication solutions that are stronger than passwords, simpler to use and less expensive to deploy and manage.

7. **Know that privacy matters**. MFA solutions can vary greatly in their approach to privacy — some track users' every move or create new databases of consumer information. Such solutions raise privacy concerns and create new, valuable caches of information that are subject to attack. Thankfully, today several authentication companies have adopted a "privacy by design" approach that keeps valuable biometrics on a user's device and minimizes the amount of personal data stored on servers.

8. **Use biometrics appropriately**. The near ubiquity of biometric sensors in mobile devices is creating new options for secure authentication, making it easier to use technology such as fingerprint and face recognition. However, biometrics are best used as just one layer of a multi-factor authentication solution — matching a biometric on a device to then unlock a second factor. Ideally, biometrics should be stored and matched only on a device, avoiding the need to address privacy and security risks associated with systems that store biometrics centrally. Any biometric data stored on a server is vulnerable to getting in the wrong hands if that server is compromised. This was the case in June 2015 with the United States Office of Personnel Management (OPM) breach resulting in 1.1 million compromised fingerprints.

Policymakers have resources and industry standards to help guide them as they address these principles. The Fast Identity Online (FIDO) Alliance has developed standards designed to take advantage of the advanced security hardware embedded in modern computing devices, including mobile phones. FIDO's standards have been embraced by a wide cross-section of the technology community and are already incorporated into solutions from companies such as Microsoft, Google, PayPal, Bank of America, Facebook, Dropbox, and Samsung.

No technology or standard can eliminate the risk of a cyberattack, but the adoption of modern standards that incorporate MFA can be an important step that meaningfully reduces cyber risk. By following these eight principles, governments can create a policy foundation for MFA that not only enhances our collective cyber security, but also helps to ensure greater privacy and increased trust online.

Michael Chertoff is co-founder and executive chairman of The Chertoff Group, a global advisory firm focused on security and risk management. He previously served as secretary of The U.S. Department of Homeland Security.

Jeremy Grant is managing director at The Chertoff Group, a global advisory firm focused on security and risk management. He previously served as senior executive advisor for identity management at the National Institute of Standards and Technology (NIST).

This article is about POLICY

⊕ **FOLLOW** THIS TOPIC

Related Topics: INFORMATION & TECHNOLOGY | TECHNOLOGY