Secure Systems

Prevention: An Enhanced Approach to Cybersecurity

Cyber crime costs the U.S. economy between $500 billion and $1 trillion a year. Cyber attacks on the country's critical infrastructure jeopardize our national and economic security, and incidents such as the recent cyber breaches at the Democratic National Committee, the Office of Personnel Management, and Sony erode the trust that Americans place in the institutions that support our way of life.

A Case for Action

Observable cybersecurity incidents have increased by more than 2000 percent since 2005.[1] They increased by 27 percent between 2013 and 2015.[2] Despite heightened awareness of cyber threats and growing expenditures for cybersecurity (which now account for as much as eight percent of the overall IT budgets at some companies), cyber attacks are likely to continue—if not increase—without a critical change in the current approach to cybersecurity.

> **"An ounce of prevention is worth a pound of cure."**
>
> –BENJAMIN FRANKLIN

Nationally and internationally, organizations largely fight cyber crime by focusing on overall baseline security. Defenders work to identify adversarial actions inside their networks, then launch counterattacks with their own targeted protections and network defense efforts. But today's determined adversaries are continually developing new ways to breach systems and establish footholds. Greatly helping them in this endeavor is the sheer volume of vulnerabilities and defects in any network that can serve as exploitable entry points. The defenders must constantly up their game to compensate for these insecure components.

Adopting a preventive strategy in the design and construction of cyber systems would represent a game-changing approach to cybersecurity. This means employing quality principles in the design and development of software and hardware in much the same way the U.S. auto industry in the 1980s applied quality principles to improve performance and lower total cost of ownership. In doing so, the government can help reduce successful attacks and conserve resources.

Instead of focusing all of our time, talent, and resources on defending subpar systems, what if we redirect a portion of investment to improve quality by design throughout the system, including foundational improvements that address quality issues at the component level?

Understanding the Problem

Many cybersecurity breaches occur through attackers exploiting software weaknesses. This quality crisis forces both software manufacturers and industry to devote costly resources to perpetually updating software to make it more secure.

Planning can begin with the use of NIST Secure Systems Engineering guidance (NIST 800-160) for improving engineering and design. It addresses the engineering-driven actions necessary to develop more defensible and survivable systems—including the components that compose and the services that

The MITRE Corporation is a not-for-profit organization chartered to work in the public interest. We apply our skills in systems engineering, research and development, and information technology to help the government address issues of critical national importance.

depend on those systems. But we need to do more to prevent losses and impact from poorly designed software-based components.

Areas of Opportunity for New Agency Leaders

Changing the process by which systems are designed and built is a huge undertaking, given how ubiquitous automation is in our lives. Right now our cyber language focuses on identifying and classifying vulnerabilities. Going forward, we need a language that specifies the level of quality assurance a software or networking product has achieved. As a major purchaser of information systems, the U.S. government can help standardize this language by specifying required quality assurance levels in the systems it buys. By doing so, the government will lay the foundation for the same approach to take hold in industry. To support a shift to a prevention-based strategy, the President should assign the following actions:

- Task the National Security Telecommunications Advisory Committee, a standing presidential advisory committee, to recommend approaches and policies to reinforce the use of prevention methods in critical infrastructures that support national security missions. This will provide a set of feasible recommendations for key industries.
- Require the U.S. General Services Administration and the Department of Defense, through public-private partnership efforts like ACT-IAC, to document effective contractual processes that use quality enumerations for software-intensive systems to ensure that the government is purchasing the highest quality software employing prevention concepts.
- Require the Office of Federal Procurement Policy to publish guidance ensuring that mission-critical programs in government leverage Common Quality Enumeration[3] in order to provide a more empirical set of data about the quality and security of software-intensive systems.
- The Office of Management and Budget should develop cost models that document the cost avoidance of improved prevention and higher quality capabilities.
- Require the U.S. Department of Homeland Security and the FBI to ensure that information sharing collaborations supported by government agencies leverage the enumerations of attacker actions documented in emerging standards such as PRE-ATT&CK™, which provides details on threat actor activities before they gain access to systems and data on networks.
- Advocate for national breach notification in order to reduce the ambiguity that currently exists across the United States with differing state-level requirements and increase the collaboration across sectors and with the relevant federal entities.
- The government should take action to accelerate the emerging cyber insurance marketplace, and evaluate its role to backstop catastrophic losses for key critical infrastructure entities.

1 Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Act of 2002, Office of Management and Budget.

2 Annual Report to Congress: Federal Information Security Modernization Act, Office of Management and Budget, March 18, 2016.

3 Software quality: A joint MITRE-SEI initiative developed a new Common Quality Enumeration (CQE) standard formally defining software quality measures which can help mitigate vulnerabilities. Already ten commercial vendors are building tools to perform automated CQE measurement and assessment.

For further ideas about applying the guidance in this paper to your agency's particular needs, email cyber@mitre.org