Report to the President:
Immediate Opportunities for Strengthening the Nation's Cybersecurity

Working Group Presentation to PCAST
November 21, 2013

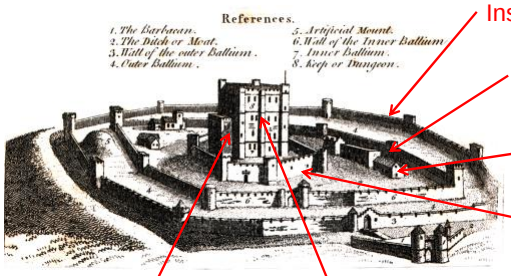
Cybersecurity Working Group:

- Craig Mundie
- William Press

Staff:

- Lauren Van Wazer
- David Pritchard

Cyberdefense once looked like this.



Institutional Firewall

Proxies and protocol checking

Port scanning

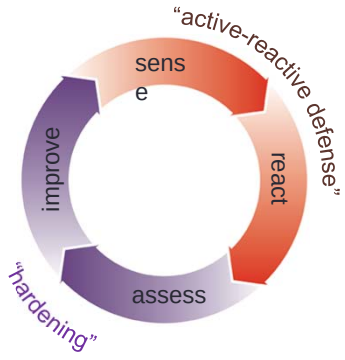
Computer configuration control

Sysadmins

Users

It was all about high walls and static defenses: "hardening"

Now, it additionally looks like this.



- Years: threat-aware software and hardware design
- Months: machine configurations, self-updating software versions
- Days: Current patches for O/S and other software
- Hours: malware signature detection and propagation
- Seconds to minutes: anomaly detection and reporting from user nodes
- Milliseconds: network attack detection, router reconfiguration or disconnection
  - in cyber conflict, national defense response

It's about processes that continuously couple threat-detection to reaction *on all timescales*.

Overarching Finding

Cybersecurity will not be achieved by a collection of static precautions that, if taken by government and industry organizations, will make them secure. Rather, it requires a set of processes that continuously couple information about an evolving threat to defensive reactions and responses.

Finding 1 addresses the Government's own cyber infrastructure.

The Federal Government rarely follows accepted best practices. It needs to lead by example and accelerate its efforts to make routine cyberattacks more difficult by implementing best practices for its own systems.

Recommendations for Finding 1

- Phase out within two years the use of unsupported and insecure operating systems, such as Windows XP, in favor of modern systems, such as current versions of Windows, Linux, and Mac OS.
- Encourage the universal adoption of the Trusted Platform Module
  - an industry-standard microchip designed to provide basic security-related functions, primarily involving encryption keys)
  - including for phones and tablets.
- Encourage the universal adoption of the latest, most secure browsers to facilitate prevention of identity theft.
- Move toward nationwide availability of proofed identities for people, roles, devices, and software.
  - While voluntary in the private sector, these should be mandatory for transactions and data exchanges among Federal users.
- Encourage effective Federal use of automatically updating software, including cloud-hosted software
  - both for COTS and GOTS products.

Finding 2 addresses regulated industries.

Many private-sector entities come under some form of Federal regulation for reasons not directly related to national security. In many such cases there is opportunity, fully consistent with the intent of the existing enabling legislation, for promoting and achieving best practices in cybersecurity.

Recommendations for Finding 2

- Within already regulated industries, the regulator should require not a specific list of cybersecurity measures but rather an auditable process by which cybersecurity best practices are adopted and continually improved.
- The President should strongly encourage independent regulatory agencies to adopt regulations that require self-reporting of continuous-improvement practices along these same lines.
  - In particular, the Securities and Exchange Commission (SEC) should mandate, for publicly held companies, the disclosure, as investment risks, of cybersecurity risk factors that go beyond current materiality tests.

This: 

NOT this: 

Finding 3 addresses the private sector.

Industry-driven, but third-party-audited, continuous-improvement processes are more likely to create an effective cybersecurity culture than are government-mandated, static lists of security measures.

Recommendation for Finding 3

For the private sector, government's role should be to encourage continuously improving, consensus-based standards and transparent reporting of whether those standards are being met by individual private-sector entities.

Finding 4 addresses private-sector sharing of cyberthreat data.

To improve the capacity to respond in real time, cyberthreat data need to be shared more extensively among private-sector entities and – in appropriate circumstances and with publicly understood interfaces – between private-sector entities and government.

Recommendation for Finding 4

- The Federal Government should act to facilitate the establishment of private-sector partnerships for the real-time exchange of threat data among potentially vulnerable private-sector entities.
  - Data flows among these private-sector entities should not and would not be accessible by the Government.
  - The Government might participate in establishing protocols, or providing technology, for how the data are utilized by the private sector for cyberdefense.
  - The protocols or technology utilized should have sufficient transparency to mitigate legitimate concerns about inappropriate Government access to private data.

Finding 5 addresses ISPs.

Internet Service Providers (ISPs) are well-positioned to contribute to rapid improvements in cybersecurity through real-time action.

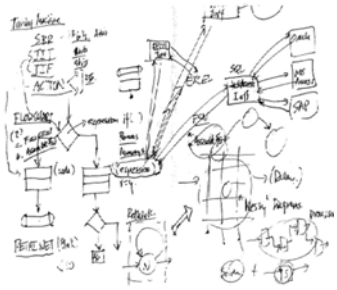
Recommendations for Finding 5

- The Federal Government should establish policies that describe the desired behavior by ISPs as best (or minimum-acceptable) practices.
- The National Institute of Standards and Technology (NIST) should work with ISPs towards establishing standards for voluntary measures by which ISPs can alert users and direct them to appropriate resources when their machines or devices are known to be compromised.

NIST

Finding 6 addresses the future.

Future architectures will need to start with the premise that each part of a system must be designed to operate in a hostile environment. Research is needed to foster systems with dynamic, real-time defenses to complement hardening approaches



Recommendations for Finding 6

- The Nation's research universities and industry laboratories should be more directly partnered in the creation of high-assurance computing systems, including hardware, firmware, and the complete software stack.
- An independent organization should be tasked with the development of certifiable maturity levels with respect to threat-aware design processes for companies that design hardware and software.
- The Nation should invest in high-risk, high-return basic research with a 10-to-20-year time horizon that, if successful, could fundamentally transform the future cybersecurity landscape.

- The Working Group recommends this report, whose full text has been previously distributed to you, for adoption by PCAST.

Thank you.