



FREQUENTLY ASKED QUESTIONS
on
CYBERSECURITY

By IEEE-USA's Committee on Communications Policy

December 2011

*This Frequently Asked Questions (FAQs) was prepared by **IEEE-USA's Committee on Communications Policy**. It represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field.*

This document does not constitute a formal position statement of the IEEE-USA, and its contents do not necessarily reflect the views of IEEE-USA, IEEE or other IEEE organizational units. IEEE-USA has issued this FAQs to enhance knowledge and promote discussion of the issues addressed.

IEEE-USA advances the public good and promotes the careers and public policy interests of 210,000 engineering, computing and technology professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity.

Introduction

There are many bills surrounding cybersecurity. IEEE-USA hopes to help the discussion by illuminating some of the technical issues around cybersecurity. Many economists, inside and outside of the government, have discussed the significant positive value a safe and secure Internet and Internet usage has on the economy. The overarching issues that underscore the importance of cybersecurity are:

- If people believe the Internet is safe, they will be more willing to use the Internet.
- If businesses believe their information and communications are secure, they will be more willing to use the Internet.
- Increased adoption of the Internet will result in continuing opportunities for existing businesses and government to reduce costs and improve efficiencies, as well as for new, innovative businesses to spring forth and help transform our economy, create jobs, and enhance our national security.

1) Why is the need for cybersecurity legislation increasing?

- Individuals: More and more people using more and more devices for more and more purposes:
 - Social networks provide more avenues for attacks and more information on victims
 - Malware, denial of service attacks, and identity theft drain resources for businesses and consumers
- Critical infrastructure: Power, water, other utilities, air-traffic control, and other elements linked to the Internet:
 - By design (“How can I as a consumer save money?”)
 - By accident (SIPRnet, Stuxnet)
- More professional attacks: Malicious teenagers; organized crime; state-sponsored attacks; rise of experienced, sophisticated cybercriminals for hire.

2) What is the root of the problems?

- No single source of vulnerabilities
- Need to consider people, process, and technology
- Lack of consequences for bad actors encourages further exploitation

- Solution space requires a multi-pronged approach:
 - Operating systems
 - Anti-virus tools and malware detection
 - Authentication
 - Self-monitoring systems
 - Cryptographic technology
 - Better training and procedures to prevent “social engineering” attacks
 - Easier to use systems to make inevitable “social engineering” more expensive and difficult

3) What type of legislative approaches have been proposed?

There are four general categories:

- 1) Prescriptive: The handbook approach. Publish “best practices,” and punish firms that don’t follow them.
- 2) Audit-based: Require firms to hire third-party “ethical hackers” to attack IT systems, detect vulnerabilities, and fix them.
- 3) Transparency-based: Require firms to disclose security breaches and compensate victims—making cost of lax security clear to company.
- 4) Insurance-based: Foster development of insurance policies to cover the cost of cyber-attacks, which would lead to insurance companies working with the companies they insure to reduce risks.

4) What effective models do we have for cybersecurity legislation?

- The security breach notification laws passed by many states have spurred companies to invest more to reduce their vulnerability to cyber-attacks.
- The U.S. government effort to address the Y2K problem is a very good model. Government did not specify how to address the problem, required detailed reports, or punished companies that were not working hard enough to fix old code. Instead, it fostered transparency, led by example by investing in fixing its own Y2K problems, and pushed government IT contractors to verify that they were addressing the problems.
- Industry-specific regulations that identify industry-specific needs, such as SEC disclosure regulations for public companies and federal and state regulations for power companies. An example of using regulations would be Y2K remediation in critical infrastructure areas, such as mandated Y2K audits of the power industry.

5) What approaches are unlikely to work?

- Building a government-only network that is not connected to the Internet
 - It is impossible to ensure that viruses and code from elsewhere aren't introduced:
 - Breach of SIPRnet and success of Stuxnet are proof-points that physically separate networks cannot solve security problems.
 - Physically separate networks are expensive and rarely provide measurable value.
 - Physically separate networks are neither redundant nor robust.
- Enforcing “best practices” in a field where the technology and type of attack change every week
- Relying on “security by obscurity”
- Prioritizing other concerns, such as illegal copying of information, in a manner that breaks the Internet model. An example of such priorities would be to corrupt basic Internet infrastructure, such as the DNS, to create short-term slow-downs to accessing of domains hosting illegal content. This would result in users bypassing legitimate DNS servers and thus render their endpoints subject to malware attack. This can result in attacks on American infrastructure from U.S. soil.
- Making IT vendors and service providers liable for vulnerabilities they could not detect or anticipate.

6) What are the most important things legislation can do?

- Foster information sharing among IT vendors and IT users (especially victims of attacks):
 - We need to leverage blogs and social media at least as well as the “bad guys.”
 - We need to enable data sharing about attacks and best practices, just as the CDC collects and analyzes data about disease and public health.
- Make the U.S. government a model customer for high-security solutions—and share lessons learned.
- Align economic incentives so firms feel the costs of lax security:
 - Breach notification laws have imposed tangible costs for data loss.
 - Note that innovation is working here. There is not a strict correlation between security spending and security: some who spend less money have more security than those who spend more. By legislating the outcome instead of the means, the market is coming up with better solutions.

- While not making IT vendors and providers liable for unanticipated vulnerabilities, ensure they are liable for gross negligence.
- Encourage companies to adopt a “transparency strategy” in addition to a security strategy and privacy policies, so that employees know what information they should be sharing (not just what information needs to be protected.) Such a strategy would focus resources on protecting the really valuable information assets, rather than trying to protect all internal information.

7) Should legislation treat different classes of companies differently?

- Efforts to distinguish between critical infrastructure and other types of IT systems will be unlikely to work. Companies that run critical infrastructure, such as utility companies and hospitals, rely upon a wide range of systems, from dedicated networks to Facebook to cellphones.
- CIOs and employees will tend to use the tools that solve their problems. However, strict regulation and audit requirements could drive them to use personal technology, rather than the “approved” and supposedly secure, but less versatile, systems.
- Special attention is needed on companies and organizations that run key parts of the IT security infrastructure (e.g., certificate authorities, providers of authentication, domain name providers). The DoC I3S category is a good start in this direction.

8) Does U.S. legislation have impacts beyond our borders?

- Many governments use U.S. legislation as a blueprint for their own legislative proposals.
- Legislation that improves transparency and information sharing could have positive, global impact.
- Investment in international “tiger teams” who can detect and respond to cyber-attacks could reduce cyber-vulnerabilities worldwide.
- On the other hand, requiring U.S. firms to follow detailed “best practices” will lead to problems if other countries are enforcing different, conflicting security standards.

9) What are potential nightmare scenarios?

- That the U.S. government, in an effort to be seen as “doing something” about cybersecurity, tries to enforce “cybersecurity checklists” based on old tools and old models of computing—slowing innovation in one of the most innovative sectors of our economy
- Worse, legislation could lead companies to implement systems and tools that compromise citizens’ privacy—without improving security
- Legislation passed in the name of cybersecurity or intellectual property protection does not have corresponding *Personal Privacy Bill of Rights* protections and *Rights of Individuals to Communicate*, per Article 20 of the UN *Universal Declaration of Human Rights*
- Legislation passed in the name of cybersecurity or intellectual property protection that structurally undermines the Internet, thereby limiting delivered security and limiting innovation for future security methods
- Legislation might encourage even more personally identifiable information (PII) collection, resulting in bigger targets and commensurately less security
- We get one-size-fits-all legislation, that puts PII and material, non-public information on the same footing as a press release, or published data sheets
- While we recognize that different agencies may have different regulations for different industries, that we end up with contradictory rules and regulations, such as differences between FCC, FTC, and local or state government rules.

IEEE-USA

2001 L Street, NW, Suite 700

Washington, D.C. 20036

+1 202 530 8332

+1 202 785 0835 fax

Web: www.ieeeusa.org

IEEE-USA Staff: *Deborah Rudolph*

E-mail: d.rudolph@ieee.org