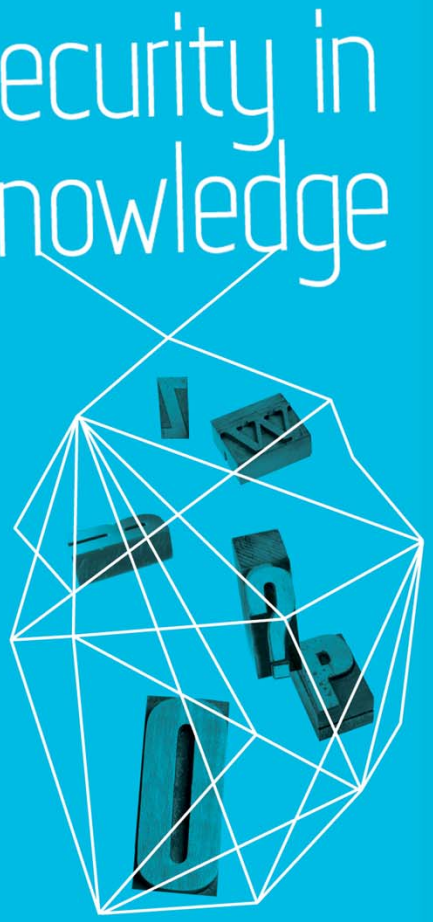
RSA CONFERENCE 2013

The Internet Health Model for Cyber Security



Kevin Sullivan
Microsoft

Session ID: PNG-T18B
Session Classification:

Think About…

What if the same were true for cybersecurity?

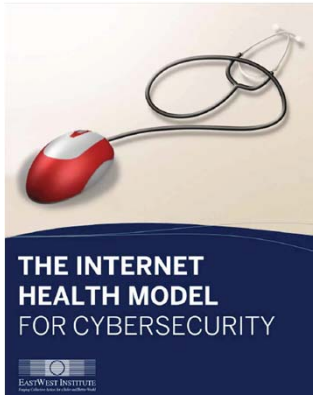
Why Look To The Public Health Model?

- Activities by both individuals and health care providers
- Guidance from organizations such as CDC and WHO
- Scientific validation of testing and treatment
- Focus on wellness and disease

Public Health Functions

Function	Application to Cybersecurity
Education	Evidence-based guidance
Monitoring	Monitoring digital networks
Epidemiology	Understand origins and impact on systems and users.
Immunization	Prevent vulnerabilities and rapidly address existing ones
Incident Response	Coordinate response to massive infections

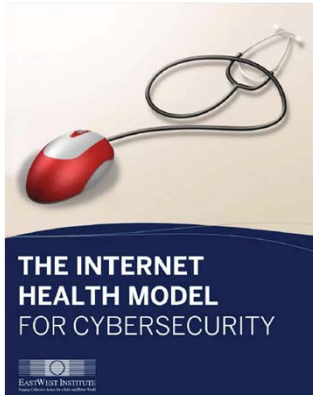
Internet Health Principles



Internet Health…

1. is a public good.
2. depends upon shared responsibility.
3. relies on evidence-based approaches.
4. emphasizes prevention over treatment.
5. is a spectrum.
6. efforts minimize potential harm.
7. efforts protect privacy.

Areas for Exploration



- Examine and address consumer expectations about security, privacy, and user control.
- **Determine how to embed targeted education and awareness opportunities into scam-resistant communications.**
- Explore the roles and responsibilities between ecosystem entities.
- Establish metrics, measurement, and information sharing schemes.
- **Explore the attributes of good health on the Internet, how that is measured, and who sets these standards.**

Targeted Authentic Communication

- Educational messages must be:
  - prioritized based on evidence of effectiveness;
  - consistent across providers and domains;
  - integrated into other elements of Internet health, including detection, notification, and remediation.

Standards for Good Health

- Remediation is complex and burdensome – how do we put more emphasis on prevention and hygiene?
- What constitutes good health online?
  - How is it measured?
  - Does it differ by country? Operating system? Personal values?
- Consumers are responsible for most internet health decisions today?
  - Should they be?
  - Do they want to be?

In Action

How to build an immune system for cybersecurity attacks

By William Jackson | Nov 08, 2012

Conclusion

- The public health model can be broadly applied to meet a range of cybersecurity challenges.
- Individuals must take ultimate responsibility for security, but an internet health system can provide a vital "safety net" to rely upon in case or emergency and for prevention.
- Model is not "all or nothing" – we should look for areas to make an impact today, inspired by the public health model.

Stay in Touch

- KevSull@microsoft.com
- Twitter: @KevSull

BACKUP

Additional Resources

- Kephart, Chess and White
  - http://www.research.ibm.com/antivirus/SciPapers/Kephart/Spectrum/Spectrum.html
- St. Sauver
  - http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf
- Charney
  - http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/02/15/advancing-the-idea-of-collective-action-to-improve-internet-security-and-privacy.aspx
- Mulligan & Schneider
  - http://www.mitpressjournals.org/doi/abs/10.1162/DAED_a_00116
- Rowe
  - http://www.crosstalkonline.org/storage/issue-archives/2012/201211/201211-Rowe.pdf

Notional anatomy of cybercrime

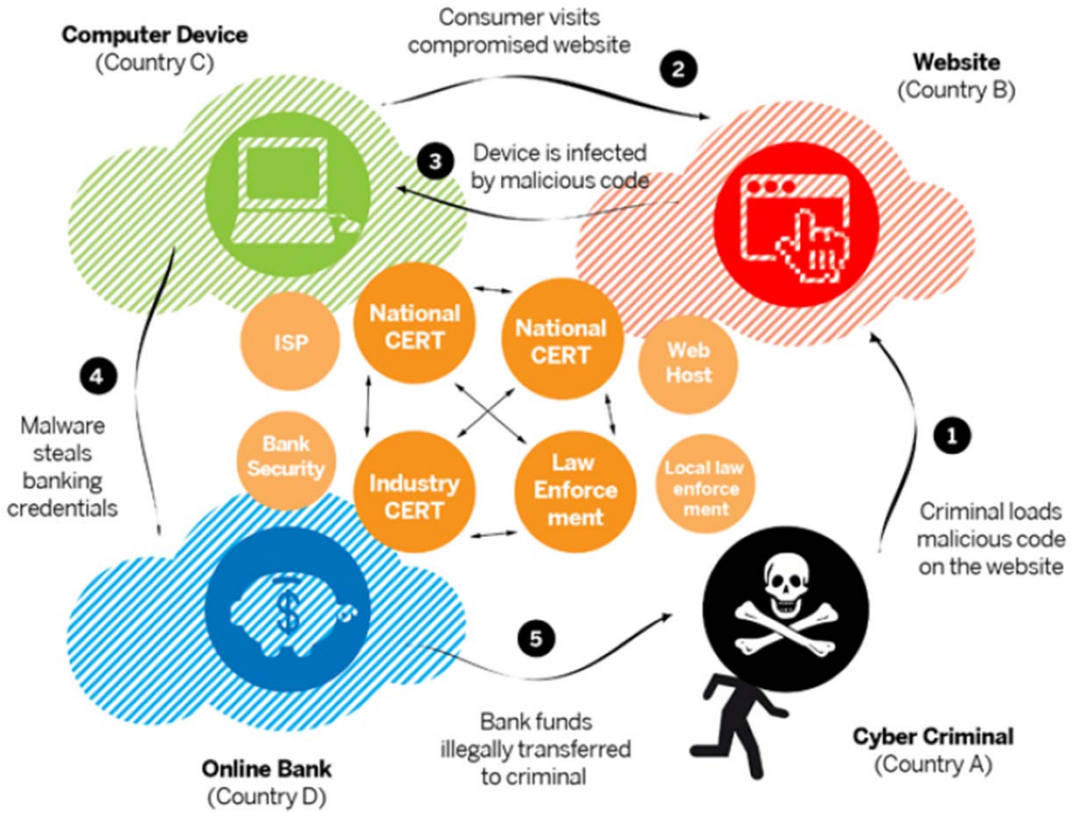


Figure 1. Anatomy of a cybercrime