CSIRTs as an Outcome of a Culture of Security

Bill Woodcock
Executive Director
Packet Clearing House

September 11, 2009

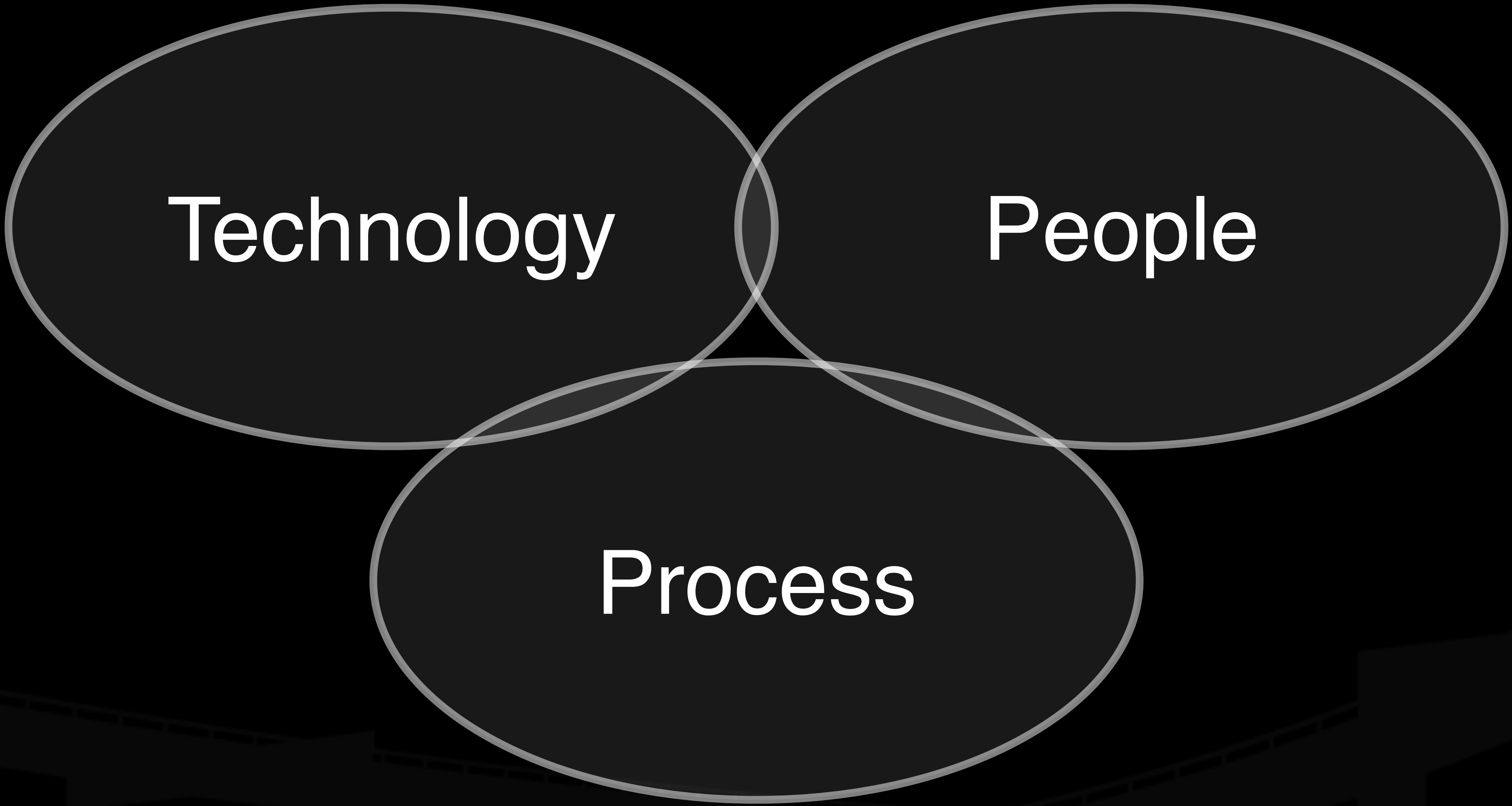
Overview

My background

Security roles and responsibilities

OECD Culture of Security and Cross-Border Cooperation framework

Culture of Security and Cross-Border Cooperation

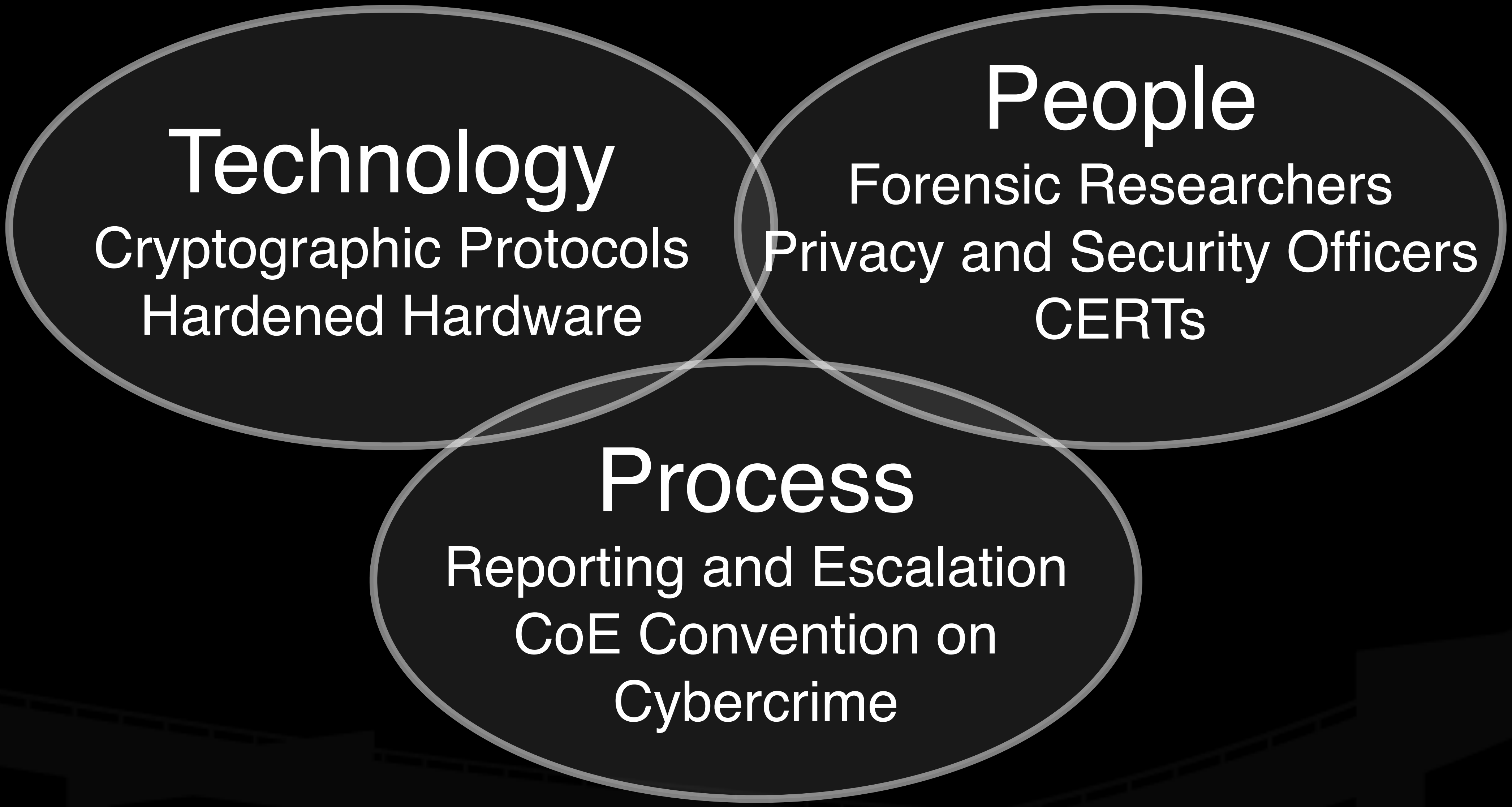


Technology

People

Process

Culture of Security



Technology

Cryptographic Protocols
Hardened Hardware

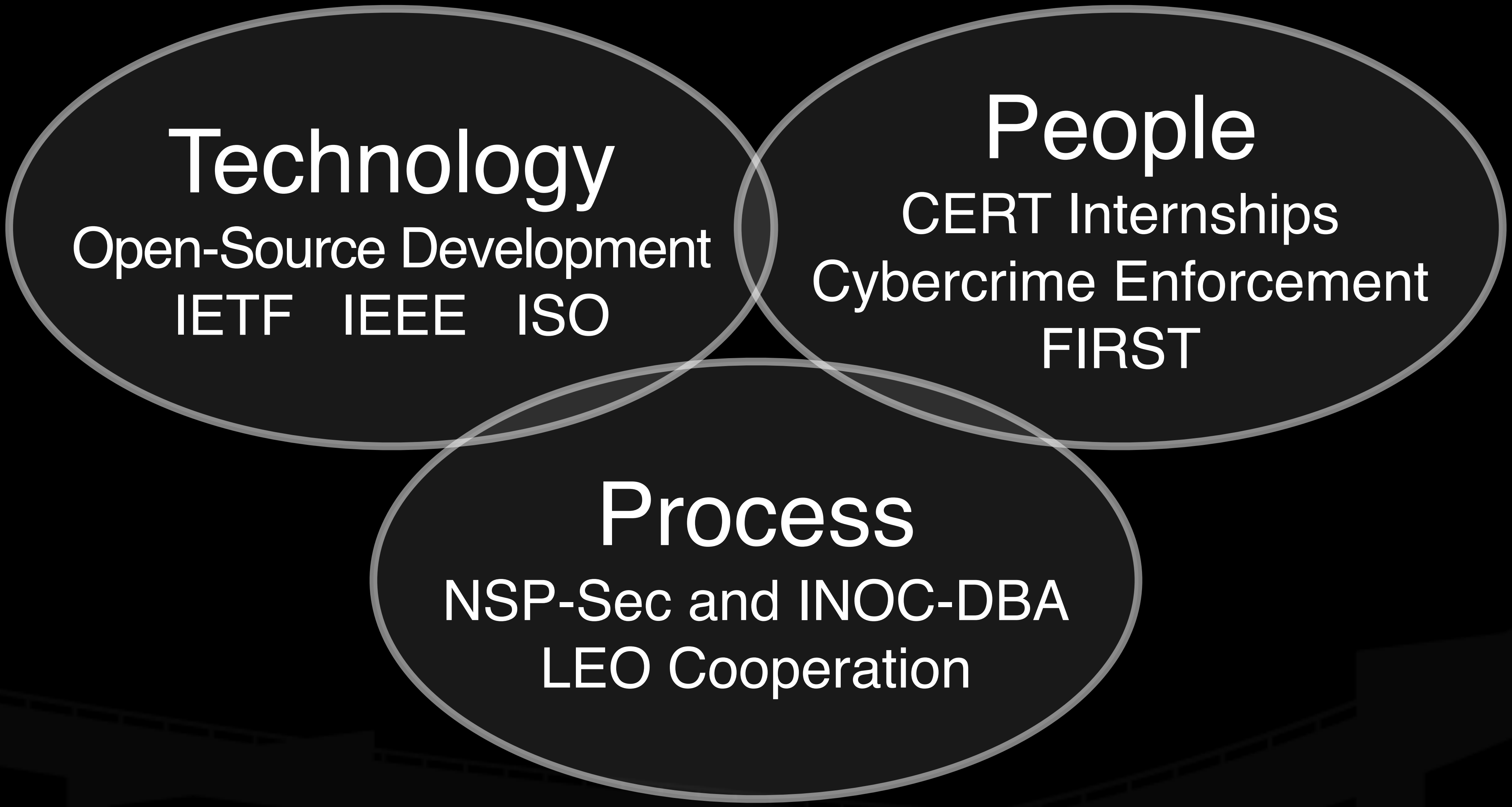
People

Forensic Researchers
Privacy and Security Officers
CERTs

Process

Reporting and Escalation
CoE Convention on
Cybercrime

Cross-Border Cooperation



Technology

Open-Source Development

IETF IEEE ISO

People

CERT Internships

Cybercrime Enforcement

FIRST

Process

NSP-Sec and INOC-DBA

LEO Cooperation

Culture: People

In order for a culture of security to exist, it must be populated.

The central institution of any culture of security is the Computer Emergency Response Team, or CERT.

New members of the culture come out of academic programs (which must be established), intern in a CERT (internationally or domestically), and go on to careers as CSOs, in CERTs, academia, law enforcement, or government.

This is fundamentally analogous to the peopling of a national health system with doctors.

Culture: Process

A culture of security, like any culture, is propagated by communication between its members, the exercise of its processes, and evangelism to people outside it.

The processes of a culture of security are, in order of declining frequency: prevention, mitigation, and prosecution.

Each of these processes, as well as outreach to those outside, are supported by the communication and coordination mechanisms that tie the society together.

Culture: Technology

The trappings and mechanisms of a culture of security are the tools and protocols that its exponents utilize in the living of their lives and the commission of their work.

Cryptographically authenticated and secured end-to-end communications protocols underly the communications of a secure culture, and defeat the ability of malefactors to violate people's privacy by eavesdropping, while hardened endpoints prevent malware like keystroke loggers and rootkits from undermining users' security and privacy. Both of these depend upon transparency and the continuous scrutiny of many security experts to test their efficacy.

These building-blocks are prerequisite to the living enactment of a culture of security.

Cooperation: People

Cooperation is enacted by people, individually or in a role representing an organization. In the case of security, the central organization is the CERT, and CERT staff are responsible for opening and maintaining the lines of communication and cooperation between the central CERT and all relevant parties.

FIRST, the association of CERTs, brings the CERTs and their staff together, to build the most fundamental links in that web of trust.

Internships and circulation of staff between CERTs and other interested organizations provides the new blood that keeps institutional knowledge and connections growing.

Cooperation: Process

International security cooperation depends upon a common frame of reference, and a common set of actions taken within that framework.

The framework is the legislative harmonization that prevents cybercriminals from arbitraging differences between jurisdictions and executing each portion of their criminal action in a jurisdiction where it’s legal, unenforced, or not extraditable.

The actions taken are defensive coordination, mitigation, and evidentiary collection and prosecution. These are coordinated through NSP-Sec and INOC-DBA, and the latter increasingly though direct LEO-to-LEO cooperation.

Cooperation: Technology

The technology of security can be measured by its openness. Only widely-published security algorithms and designs can be trusted, since they’ve been tested by many people, and scrutinized by many experts.

The vast majority of the open-source tools used by the security community are developed in academia, or in the open standards organizations: the IETF, the IEEE, and ISO.

These mechanisms are inherently international, but are also more easily afforded and supported by wealthier developed countries. Knowledge transfer about OSS tools is thus an obligation of those wealthier countries, since OSS doesn’t have a marketing budget.

Culture and Cooperation

In conclusion, the two most important concepts:

A continuous flow of newly-educated security experts must enter the workforce, from academia, through CERTs, and out to industry and government, or recursively back into senior positions in academia and the CERTs.

Prevention is better than mitigation, and many more incidents will be mitigated than will ever be prosecuted. A hierarchy of triage must be followed that does not privilege mitigation over prevention in the first place, nor privilege evidentiary preservation over mitigation.

Thanks, and Questions?

Copies of this presentation are available in PDF format.

Bill Woodcock
Executive Director
Packet Clearing House
woody@pch.net
+1 415 831 3103