CAN VENDORS EVER PROVIDE SECURE SOLUTIONS?

Barry Greene - bgreene@senki.org
The Short Answer ......

NO
"[T]he malware that was used would have gotten past 90 percent of the Net defenses that are out there today in private industry and [would have been] likely to challenge even state government,"

Joe Demarest, Assistant Director - US FBI’s Investigation’s Cyberdivision.

What this is really saying is that when there is a will, there is always a way to violate a system.
Our Traditional View of the World

The Internet is not organized based on countries. It is a group of “Autonomous System Networks” (ASNs) all interconnected in a Global Network.
How does a government enforce the rule of law where the Internet’s risk are all trans-national?
Miscreant - Incident Economic Cycles

These Cycles Repeat

Incidents

Activity Peak

Lots of Problems & Attacks

Community Mitigation

Survive the Next Attack

Miscreant & Criminal R&D

New Criminal Revenue Opportunities

Resolve the Problem

Drive the Post Mortem

Trough

Expansion

Drive the Preparation

These Cycles Repeat
Work on the Right Security Problem

The Good Guys are the Big Part of the Security Problem

This is nice to know

Who we need to Target
Threat Vectors have Evolved

Corporate Threats (New!)
The dialog between US & China will accelerate the corporate on corporate threat vector.

Cyber-Criminal Threats
Cyber-Crime is an International Legal problem that has no short term resolution. There will always be someplace in the

Nation State Threats
Post-Snowden, the secret world of nation state security is now all in the open. Your network is a valid “Battle Space” for any Cyber-War.

Political, Patriotic, Protestors
There are always going to be someone, somewhere, who is upset with society - with the ability to make their anxiety know through any network - any where.
What really happens if I’m attacked?

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
The market does not penalize!

The “market” is forgiving IF you have a security reaction plan.

A security reaction plan will not prevent revenue losses, customer churn, and legal actions, but … organizations do recover from “big data breaches”
Liability “Should be” Flowing Down Hill
Think of the current and future security threats as a force of nature we live in. This is not new to human society. We have to live with the issues of nature all the time.

Like a hurricane, it is not a matter of if, but when. Even worse, you can be in a zone where the hurricane, tornado, flood, earth quake, and blizzard are all a major risk.

Forces of Nature cannot be stopped - the only thing you can do is mitigate risk through your design, preparation, and investment.
Key Takeaways ......

- If the threat vectors are not going away, then the risk will be persistent for the next few DECADES!

- If the market does not penalize companies for the major security violations, then there are no “market forces” to drive major security improvements.

- The massive growth in the “security eco-system” is driving decision makers into no action. They are not sure what really needs to be done.

- Vendors are not being help up as liable to security risk. This means there normal capitalistic forces that drive for change.

- Thinking of security as a “force of nature” is a more appropriate way of considering the real risk security threats have on the business and society.
Driving Change through “Vendor Conversations”
Checklist Approach

- Checklist are one of the most essential tools for productivity we have in the industry.
- Surprisingly, too few “Internet” and “Telecom” operators use the checklist approach to optimize their operations.
- What follows is the first in several “check list” designed for Internet Service Providers, be they Mobile, traditional Telco, Content, or ISPs.
- They can be cut/pasted and used in your organization.
- Additions to the checklist are always welcomed.

Note: If this is new to you, read the book “The Checklist Manifesto” and watch the TED talk:

http://www.ted.com/talks/atul_gawande_how_do_we_heal_medicine

* Thanks to Stephen Stuart @ Google for pointing out Atul Gawande’s book
Check for the Operator’s Conversation

- We have lots of standards, compliance guidelines, and certifications.

- What is missing is a tool to assist the operator to have a meaningful security conversation with their vendors.

- These “conversations” help the operator understand the real security maturity of their vendors. This in turn helps them determine risk within their business.

- These “security conversations” ARE NORMAL ENGINEERING DISCIPLINE! Vendors who push back on the security conversation are expressing to your and your organization their real views of “security.”
General Principles

- Set up regular meetings with your vendors to have these conversations.

- Get responses in writing from your vendors. The writing process is not a burden for the vendor. The questions asked in the checklist applies to all their customers. Every question asked is a question that would be asked by other customers.

- Do not expect perfection. No vendor has everything covered. There are always big gaps.

- Ask for the vendor’s resolution plan. How will they fill the gap. Some gaps may take a long time to rectify, which is OK if the vendor is committed to change.
Phase 1 - Review the Vendor’s Vulnerability Management Process

- Does the Vendor have a Vulnerability Management Process?

- Check the vendor’s website. See if they have a “/security” page with information about how to report a security vulnerability and their security team.

- Check the vendor’s website. See if they have a “/security” page with information about how to report a security vulnerability and their security team.

- Does the vendor have a Security and Vulnerability Response Team that is available 7x24, 365 days a year with English as the primary language of business?
Phase 1 - Review the Vendor’s Vulnerability Management Process

- Does the vendor participate with industry vulnerability and incident response teams?
- Does the vendor participate with the national vulnerability and incident response teams?
- How would the vendor notify our organization about a security vulnerability?
Phase 2 - Review the Vendor’s Security Development Lifecycle

- How is the vendor’s SDL integrated into the vendor product development processes?
- How does the SDL process allow for rapid vulnerability fixes?
- Does the SDL process used a form of Root Cause Corrective Action (RCCA)?
- Does the vendor’s SDL include regular Static Analysis Testing?
Phase 2 - Review the Vendor’s Security Development Lifecycle

- Does the vendor use Test Driven Development (TDD) in their software deployment?
- Does the vendor use Dynamic Analysis Testing (DAST) in the vendor’s development process?
- Does the vendor use the industry vulnerability classification and enumeration tools? (CVE, CWE, etc)
- Does the vendor have Regression, Stress, Performance, and Compliance System Testing?
Phase 2 - Review the Vendor’s Security Development Lifecycle

- Does the vendor use of fuzz testing in their quality processes?
- Does the vendor have documented risk assessments for all elements, protocols, systems, and solutions?
- Does the vendor use specific security testing tools for their Unit Under Test (UUT) testing?
Phase 3 - Review the Vendor’s Healthy Interaction & Transparency

- Will the vendor’s Security and Vulnerability Response Team review postmortem on past vulnerabilities with our organization?
- Does the vendor bring in 3rd party penetration test and security auditors?
- Will the vendor be open to a joint table top exercise?
- Will the vendor be willing to open their code to an operator driven source code audit?
Phase 3 - Review the Vendor’s Healthy Interaction & Transparency

- Will the vendor publish the “reporter” of a security vulnerability in their security advisory?
- Does the vendor have an active bug bounty program?
- Will the vendor provide the required GPL documentation based on request for all open source software used in the organization?
- How does the vendor manage open source security vulnerabilities?
What is Next?

- Phase 4 Conversation - Joint Reaction Plans
- Phase 5 Conversation - Review Industry Certification
- New items to be added:
  - How does the vendor protect their network? For example, how does the vendor protect their signing keys?
  - How can a vendor help during an attack (vs a vulnerability disclosure)?
  - What should the organization do to “plug in” to the vendor’s security processes?
Partnership between Vendor & Operator

Quality Chain

- Regression Testing
- Security/Resiliency Testing (Negative & Fuzz Testing)
- Engineering Delivers Code
- Sys Test (Positive Testing - Compliance, Systems, and Unit)

Vendor

- Software Released
- Support Replication
- Support Ticket
- Security/Resiliency Testing
- Security Team TRIAGE Evaluation

Operator

- Customer Security Test Software w/ Commercial Tester
- Customer Test Software
- Customer Uses Software
- Software Breaks
- Potential Vulnerability

Additional Tests:
- Post Release Hardening & Performance Testing
- Security/Resiliency Testing (Negative & Fuzz Testing)
- Network Operator
- Security/Support Proactive Testing
- Regression Testing
- TRIAGE Evaluation
- Potential Vulnerability
Your Turn ....

✓ Commit to do something to prepare your organization. Have the Conversations with the Vendors.

✓ The “Conversations” = “Customer Requirements” which drives change in the vendor’s priorities.

✓ Where to get the “Checklist?”

  ➡️ www.senki.org

  ➡️ Barry’s Linkedin Post - http://www.linkedin.com/in/barryrgreene/ or Twitter: @BarryRGreene