Staying Ahead of the Security Poverty Line
(or just getting ahead in the first place)

Andy Ellis
Chief Security Officer

@csoandy
#HITB2012AMS
Security Poverty Line

Organizations that don’t have enough resources to implement perceived basic security needs.
Security Poverty Line

Organizations that don’t have enough resources to implement perceived basic security needs.

Security Subsistence Syndrome
“I can’t even do the barest minimum to cover my ass, so I’d better not do anything but cover my ass.”
Security Poverty Line

Organizations that don’t have enough resources to implement perceived basic security needs.

Security Subsistence Syndrome
“I can’t even do the barest minimum to cover my ass, so I’d better not do anything but cover my ass.”

Accruing Technical Debt
With every step forward, the undone work increases risk and makes future steps harder.
Adding value: “measuring” a security program

\[ \text{Value} = \text{resources} \times \text{capabilities} \]
Adding value: “measuring” a security program

Value = resources * capabilities

time + money
Adding value: “measuring” a security program

Value = resources * capabilities

time + money  skill * effort * effectiveness
How much security is “good enough”?

Security value
How much security is “good enough”?

- “Good” security

Security value
How much security is “good enough”?

- "Good" security
- Sufficient against the casual chaotic actor
How much security is “good enough”?

- What you need to fend off a nation state
- “Good” security
- Sufficient against the casual chaotic actor
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- “Good” security
- Sufficient against the casual chaotic actor
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you
- “Good” security
- Sufficient against the casual chaotic actor

Security value
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you
- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you
- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
- Enough to fool the standard auditor
How much security is “good enough”? 

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you
- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
- Enough to fool the standard auditor
- What your organization thinks it can get away with
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you
- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
- Enough to fool the standard auditor
- What your organization thinks it can get away with
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you

- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
- Enough to fool the standard auditor
- What your organization thinks it can get away with
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you

- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
- Enough to fool the standard auditor
- What your organization thinks it can get away with

Security value
How much security is “good enough”?

- “Perfect” security
- What you need to fend off a nation state
- Where a good assessor can help you

- “Good” security
- Sufficient against the casual chaotic actor
- Enough to convince a serious auditor
- Enough to fool the standard auditor
- What your organization thinks it can get away with
HD Moore’s Law

Sufficient against the casual chaotic actor

A rising tide lifts all boats...
HD Moore’s Law

Sufficient against the casual chaotic actor

A rising tide lifts all boats…
HD Moore’s Law

Sufficient against the casual chaotic actor

A rising tide lifts all boats...
HD Moore’s Law

Sufficient against the casual chaotic actor

A rising tide lifts all boats...
HD Moore’s Law

Sufficient against the casual chaotic actor

A rising tide lifts all boats...
Peltzman Effect

What your organization thinks it can get away with
Peltzman Effect
What your organization thinks it can get away with
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Perceived risk

Security value

Thursday, May 24, 2012
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Perceived risk

Security value
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Security value

Perceived risk
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Perceived risk

Security value
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Security value

Perceived risk
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Perceived risk

Security value
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Perceived risk

Security value
Set-point theory of risk tolerance

Tolerance of perceived risk drives to a stable equilibrium

Perceived risk

Security value
Perceived Risk vs. Actual Risk
Perceived Risk vs. Actual Risk

perceived

actual

undisclosed breach
Perceived Risk vs. Actual Risk

- Perceived
- Actual

- Known vulnerability
- Undisclosed breach
Perceived Risk vs. Actual Risk

- Perceived Risk
- Actual Risk

- "FUD"
- Known Vulnerability
- Undisclosed Breach
Perceived Risk vs. Actual Risk

- Perceived
- Actual

- "FUD"
- Known vulnerability
- Undisclosed breach
- Stealth improvements

Thursday, May 24, 2012
Perceived Risk vs. Actual Risk

- Perceived
- Actual
- "FUD"
- Known vulnerability
- Undisclosed breach
- Stealth improvements
- Risk reduction
Perceived Risk vs. Actual Risk

- Perceived
- Actual

- Stealth improvements
- Risk reduction
- Security theater
- "FUD"
- Known vulnerability
- Undisclosed breach

Thursday, May 24, 2012
Don’t beg for money ...
Don’t beg for money ...

Utah CTO takes fall for data breach
Resignation sought by Gov. Herbert after breach exposes data on 280,000 Medicaid recipients
Don’t beg for money ...

Utah CTO takes fall for data breach
Resignation sought by Gov. Herbert after breach exposes data on 280,000 Medicaid recipients

“We need to roll out FDE immediately! And DLP!”
Don’t beg for money ...

Utah CTO takes fall for data breach
Resignation sought by Gov. Herbert after breach exposes data on 280,000 Medicaid recipients

“We need to roll out FDE immediately! And DLP!”

WikiLeaks, Pirate Bay suffer DDoS attacks, back online

“We need DDoS protection, right away!”
Don’t beg for money ... 

Utah CTO takes fall for data breach
Resignation sought by Gov. Herbert after breach exposes data on 280,000 Medicaid recipients

“We need to roll out FDE immediately! And DLP!”

WikiLeaks, Pirate Bay suffer DDoS attacks, back online

“We need DDoS protection, right away!”

Hackers break into Azerbaijan Eurovision websites

“And a WAF! And someone to look into our coding practices!”
... instead waste your crises ...

- And of course last but not LEAST a special From AKAMAI technologies yes sireee
- (you guys cant keep this kind of stuff under wrapps)
- (yes what if someone mass executed ping -f 6500 yahoo.com from your noc)
- (i dont think anyone could block 5000+ machines world wide)
- --

- --------@athena.dialup.mit.edu's password: luxlaczconcaprevesiebsmdakanetwork24sdoyo
- Got RSA key from '-----@crabcake.kendall.akamai.com' to macau.nocc.akamai.com with pass h4rdc0r3
... and effect long term change

What if you found an organization where every developer had a copy of the key used to gain root access to every production system?

On their desktop?

At home?

How would you fix this?
Security Awareness

The Problem:
• Auditors believe that if we just train everyone with a basic security education, then *of course* we’ll have no problems!

The Solution:
• Basic, standard security awareness, web-based, automated, simple.
• Targeted training, not exposed to auditors.
Security Awareness

The Problem:
• Auditors believe that if we just train everyone with a basic security education, then of course we’ll have no problems!

The Solution:
• Basic, standard security awareness, web-based, automated, simple.
• Targeted training, not exposed to auditors.

Security Awareness

Your Action
Click the button near the bottom of the page to track two things. First, that the Information Security Policy and Program has been made available to you, and that you have read and understand how these policies apply to you. Second, that you have received security awareness training (this page), with access to more information as desired.

Continue to safeguard Akamai, and our customers, against the threats to our information assets. Your responsibility doesn’t end with this web page.

Your Responsibilities
Akamai, as a provider of application acceleration services, frequently transports, processes, and stores information of value to our customers and their users. We have been placed in a position of trust - our customers expect that we will respect the confidentiality of this data, whether it is a pay-per-view stream, health care information, a credit card transaction, or simply their usage information. As part of your job, you may have administrative or technical access to this content or to configuration which controls this content. This position of trust requires diligence and care in protecting the rights of others from security breaches.

Part of that diligence is understanding your role in Akamai’s security. Read the documentation linked below and follow the training provided. If you have any questions, please contact your manager or InfoSec.

Security Importance
Every day, each employee at Akamai interacts with sensitive information, security process, or critical systems. These systems may control the flow of large portions of Internet traffic, or transmit credit card holder data, or reveal how our customers utilize Akamai for competitive business advantage. The purpose of regular security awareness training is to ensure that employees are considering the importance of protecting these assets each and every day, and are aware of the security assets available to them.

Akamai is committed to a strong security program and posture, not only by meeting our customers’ requirements, but by following industry standards and regulations such as ISO 17799/27001 (the Code of Practice for Information Security Management), the Payment Card Industry Data Security Standard, and NIST 800-53, among others.

Security Training Available
Akamai generally provides targeted training throughout the year, rather than one, multi-hour sit-down session each year. We’ve collected those resources here so that you can use this page as a reference and a refresher course in security.

Beginning with the Security Orientation, which provides an initial, comprehensive overview (and is always a decent refresher), employees may also receive targeted security awareness training, such as the Social Engineering Training. Periodically, important security and ethical topics are brought up via email, in cross-functional meetings, or at quarterly all-hands meetings.

Employees also have access to the Information Security Policy (2 pages) and the Information Security Program (72 pages), which provides a set of guidance on a broad range of information security topics; other security policies can be found on the security policy page. Additionally, targeted security training and information is provided upon request to organizations across the business.

Protected Data
Some types of data require special handling for either legal or compliance reasons. These include:
• Protected Health Information, protected under HIPAA (the Health Information Portability and Accountability Act)
• Credit Card Data, covered by the PCI DSS (Payment Card Industry Data Security Standard)
• Billing Information, subject to audit under SOX (Sarbanes-Oxley)

If you are working with such data, please follow the required procedures and protocols. If you have any questions, you can contact your manager or infosec inside@akamai.com.

Why this page?
In addition to making security important to our business, we must ensure that every employee, annually, not only has received security awareness training, but that we document that training, and that they have the Information Security Program made available to them. This page is designed to raise your awareness of customer security needs, as well as make various training and policy materials available to you. Please follow the links and read and understand our security program here at
The Problem:
• Auditors believe that if we just train everyone with a basic security education, of course we’ll have no problems!

The Solution:
• Basic, standard security awareness, web-based, automated, simple.
• Targeted training, not exposed to auditors.
Security Awareness

The Problem:
• Auditors believe that if we just train everyone with a basic security education, then of course we’ll have no problems!

The Solution:
• Basic, standard security awareness, web-based, automated, simple.
• Targeted training, not exposed to auditors.
Third party security reviews
Third party security reviews

Define requirement
Third party security reviews

- Define requirement
- Evaluate vendors
Third party security reviews

Define requirement → Evaluate vendors → Select vendor
Third party security reviews

Define requirement → Evaluate vendors → Select vendor → Implement solution
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

Security evaluation

Thursday, May 24, 2012
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

Security evaluation
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

Security evaluation

Thursday, May 24, 2012
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

Security evaluation

Security evaluation

Security evaluation

Security evaluation

Thursday, May 24, 2012
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

- Security evaluation
- Vendor Hell
- Security evaluation
- Security evaluation
Third party security reviews

- Define requirement
- Evaluate vendors
- Select vendor
- Implement solution

Security evaluation
Vendor Hell
Auditor CYA
Security evaluation

Thursday, May 24, 2012
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

- Security evaluation
- Vendor Hell
- Auditor CYA
- Scapegoat hunt
Third party security reviews

1. Define requirement
2. Evaluate vendors
3. Select vendor
4. Implement solution

- Business alignment
- Vendor Hell
- Auditor CYA
- Scapegoat hunt
Hunting for malware in a 10PB cloud

http://bitly.com/AkaVscan
Hunting for malware in a 10PB cloud

http://www.flickr.com/photos/james_lumb/3921969141/

http://bitly.com/AkaVscan
How easy is juggling?
How easy is juggling?
How easy is juggling?
How easy is juggling?
How easy is juggling?
Takeaway: Measuring security value

Value = resources * capabilities

time + money

skill * effort * effectiveness
Takeaway: Measuring security value

Value = resources * capabilities

time + money

skill * effort * effectiveness

Goal of any security program: dv/dt > 0
Takeaway: Measuring security value

\[
\text{Value} = \text{resources} \times \text{capabilities} \times \left( \text{time} + \text{money} \right) \times \text{skill} \times \text{effort} \times \text{effectiveness}
\]

Goal of any security program: \( \frac{dv}{dt} > 0 \)

Below the Security Poverty Line, we see Security Subsistence Syndrome: relying on \textit{resources}, not \textit{capabilities}.

Goal: \( \frac{dr}{dt} > 0 \)
Takeaway: Measuring security value

Value = resources * capabilities
time + money  skill * effort * effectiveness

Goal of any security program: $dv/dt > 0$

Below the Security Poverty Line, we see Security Subsistence Syndrome: relying on resources, not capabilities.
Goal: $dr/dt > 0$

A good security program wants to create surplus.
Goal: $dc/dt > 0$
Questions, Answers, and Pontifications

Andy Ellis
aellis@akamai.com
@csoandy
http://www.csoandy.com/