BLUEBOX

STRATEGIES FOR SECURITY: WHEN, WHY, HOW

Adam Ely

adam@bluebox.com

www.bluebox.com

@BlueboxSec

ABOUT ME

Experience

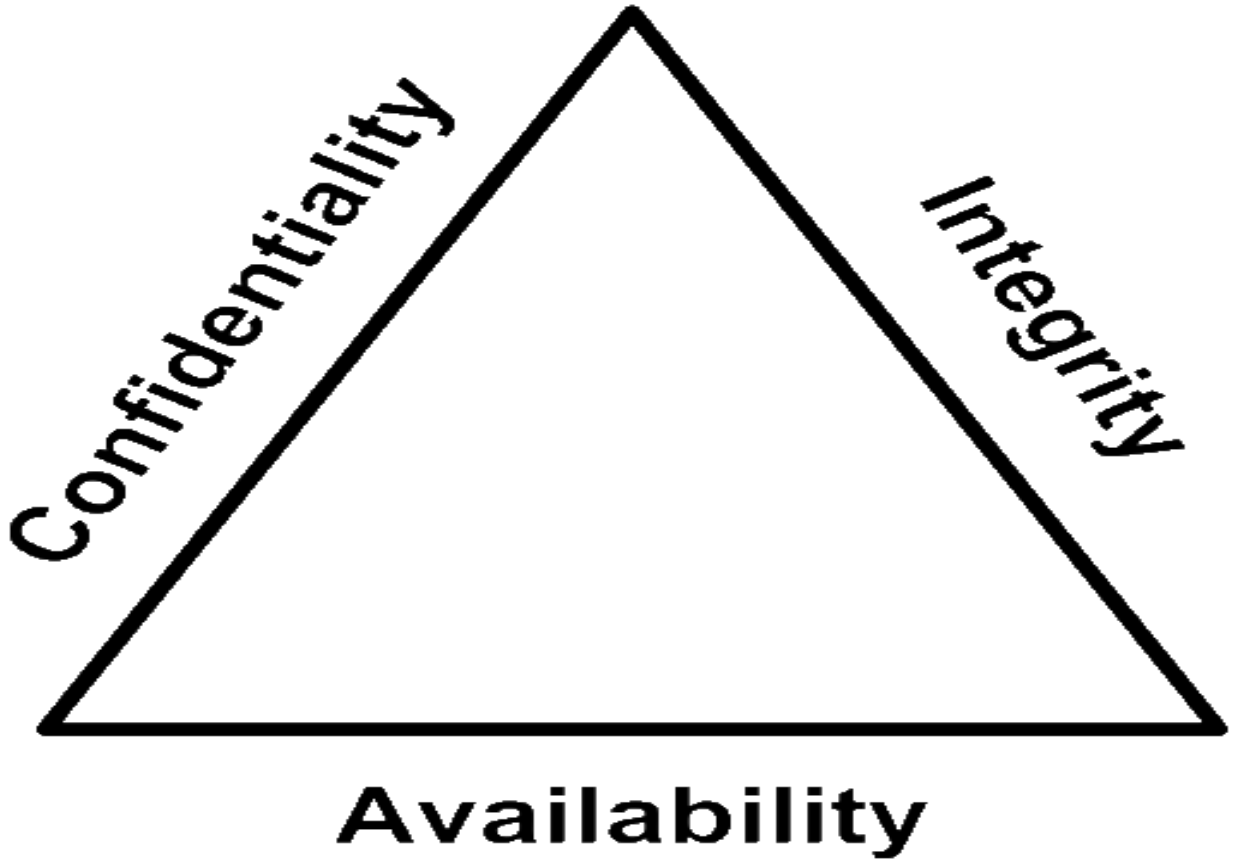
- Co-founder Bluebox Security
- CISO, Heroku
- CISO, TiVo
- Walt Disney….

Other nifty stuff

- Coded exploits
- Consulted for the government
- Published numerous articles & papers
- <insert other egotistical stuff here>

DEFINE: SECURITY

CIA Triad: Use as a basic guiding principle



DEFINE: SECURITY

Security is comprised of many things.

- Technical bits
  - Application security
  - Infrastructure security
  - Access controls

- Non-techie bits
  - Process
  - Compliance
  - Legal
  - Assurance

DEFINE: SECURITY

Security is comprised of many things.

- Technical bits
  - Application security
    - Code standards
    - Sanitization functions
    - Vetted framework versions
    - Application/lib/framework updates
    - Logging
    - Session handling
    - etc….

DEFINE: SECURITY

Security is comprised of many things.

- Technical bits
  - Infrastructure security
    - Configuration
    - Hardening
    - Patching
    - User & group management
    - Network topology/security groups
    - Logging
    - etc….

DEFINE: SECURITY

Security is minimizing risk to both those that trust us and our organization through the assurance of confidentiality, integrity, and availability.

I’m embarrassed to even mention the triad but it works and proves this shit ain’t new.

SECURITY: WHY

- Bullshit answer
  - Compromises always mean loss of business
- Crappy answer
  - Depends on your business
- Better Answers
  - Spike Lee said: Do the right thing
  - You have IP that is valuable, don't get jacked
  - Customers have valuable information
  - Dealing with fines & bad publicity is a PIA
  - Enterprises need assurances

SECURITY: WHY

Enterprises need assurances. Why?

#1 Reason

- You haven't proven yourself as being legit and on their level. Much like dating.

Other

- Valuable assets = loss of market leadership
- Monetary penalties = no return on this "investment"
- Someone's ass is on the line = Bob gets fired

SECURITY: WHY

But what do I get from security?

- Customer adoption
- Market leadership
- Money ($$$$$)

DEFINE: HOW

- Make it frictionless and part of how you operate
- Understand customer concerns
  - Distinguish between needs and wants
- Understand your risks & concerns
- Prioritize
  - Big wins first
  - Just like building a product
- Learn from those before us
- Define ownership
- Communicate & be transparent

DEFINE: HOW

Make it frictionless and part of how you operate

- If it interferes with productivity, people will ignore it, go around it, and bitch about it.
- Build security into what you already do
- Give good options for doing the right (secure) thing.

Example: Have a custom client side tool? Have it perform a client side audit each time it runs. Continuous auditing w/o manual audits

DEFINE: HOW

Understand customer concerns

- Customers want everything
- Boil down to what they need
- Solve for need, work towards want

Example: Customer might want PCI compliance. Not relevant to your business? Show intent and how you meet their data security needs while working to check that box for future clueless customers.

DEFINE: HOW

Understand your risks & concerns

- You know your risks better than anyone
- Where do you think you have issues?
- How would you exploit those weaknesses?
- How easy would it be for someone else?
- Define and prioritize

DEFINE: HOW

Prioritize

- What can you do now that gives the biggest wins?
- Security prioritization is just like building a product
- Think of a CISO as the product manager of your security

DEFINE: HOW

Learn from those before us

- This shit ain’t new
- Learn from previous breaches
- You’re smart but this isn’t your wheelhouse
- RTFM, plenty of resources out there

DEFINE: HOW

Define ownership

- Executive level champion to influence the org.
- Tactical level leaders and involvement to keep it fresh and moving

DEFINE: HOW

Communicate & be transparent

- Ease customers minds, communicate
- Document what you do, say what you don't
- Show that you're always working to be "better" and meet their ever changing needs
- Build a transparent relationship
- Find the right verticals, go after others when ready

DEFINE: HOW

Where to actually start?

- Customer data storage and handling
- Culture of treating security as a first class citizen
- Customer data storage and handling
- Application security
- Infrastructure configuration & patching
- Access controls
- Policies/documentation
- 3rd party audits

SECURITY: WHEN

- Start as early as possible
  - Make it core to the culture
  - The sooner, less to fix later
- Increase effort as needed to meet customer needs/demands
- Roadmap your security strategy like a product
- Hire dedicated people for security when you must impress customers, there is no forward momentum, or there is work to justify doing so
- Prior to that, involve anyone who wants to help

BLUEBOX

STRATEGIES FOR SECURITY: WHEN, WHY, HOW

Adam Ely

adam@bluebox.com

www.bluebox.com

@BlueboxSec