CSSF

Common Sense Security Framework

Common Sense Security Framework

Jerod Brennen, CISSP

CTO & Principal Security Consultant, Jacadis

Agenda

<rant>

Bad Things Are Going To Happen

Image from http://www.buzzfeed.com/daves4/definitely-dead

You Know Your Business

- Company culture
- Day-to-day operations
- Balancing revenue vs. expenses
- Meeting customer expectations
- Standing out among your competitors

- True for large corporations and small businesses
    - Global economy
    - Depend on one another

Small Business Numbers

- Small businesses make up:
  - 99.7 percent of U.S. employer firms,
  - 64 percent of net new private-sector jobs,
  - 49.2 percent of private-sector employment,
  - 42.9 percent of private-sector payroll,
  - 46 percent of private-sector output,
  - 43 percent of high-tech employment,
  - 98 percent of firms exporting goods, and
  - 33 percent of exporting value.

From https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf

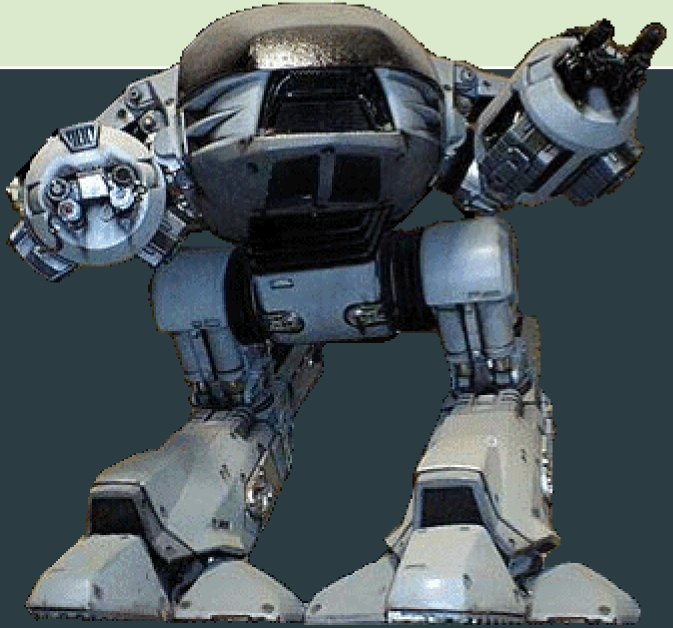
But More Importantly…

- How we pay our bills
- How we feed our families
- How we put our kids through school
- How we afford to live the lives we're trying to live

One Size Security Does Not Fit All!

You Have 20 Seconds to Comply!

Standard	Number of Controls
PCI DSS 3.0	228 controls
NIST SP 800-37 (FISMA)	204 controls
SANS 20 Critical Controls	197 controls
ISO 27002:2013	114 controls
ASD Strategies to Mitigate Targeted Cyber Intrusion	35 controls (confidentiality only)



Unified Compliance Framework

- Authorities Document List
  - 650+ (at my last count)
- 25,000+ citations mapped to ~3,500 controls
- Annual subscriptions, ranging from $1k (individual) to $20k (corporate)

Information Overload

Let’s Take a Step Back…

Look Familiar?

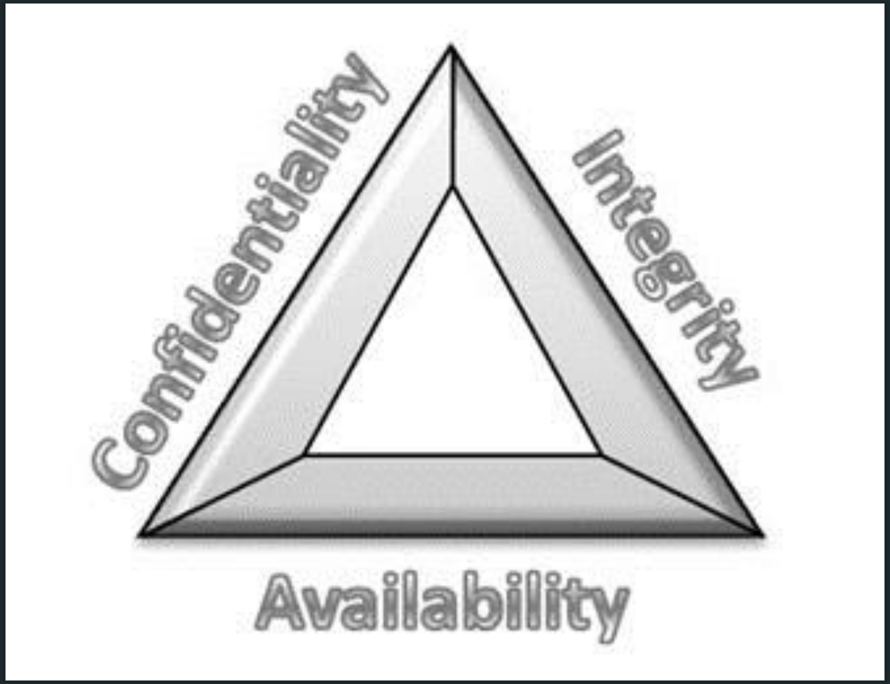


Image from http://i.technet.microsoft.com/dynimg/IC24247.jpg

How About This?

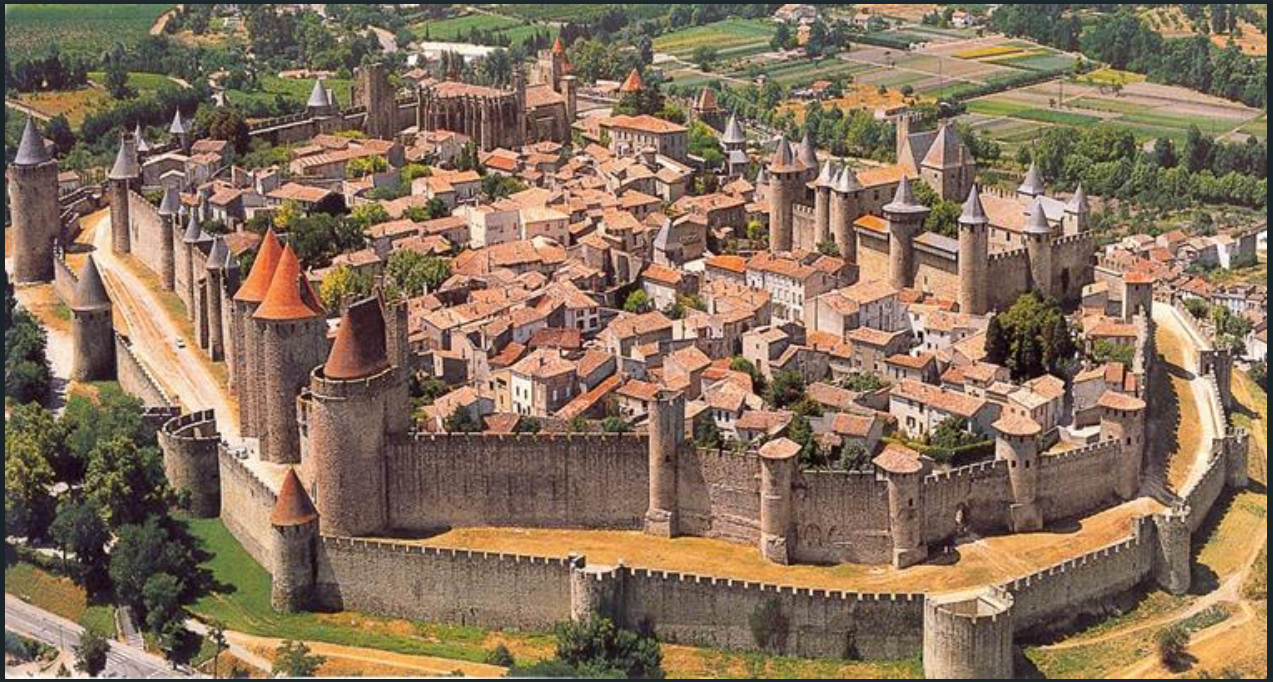


Image from http://www.creme-de-languedoc.com/_images/tourism/carcassonne/2.jpg

Another One?!

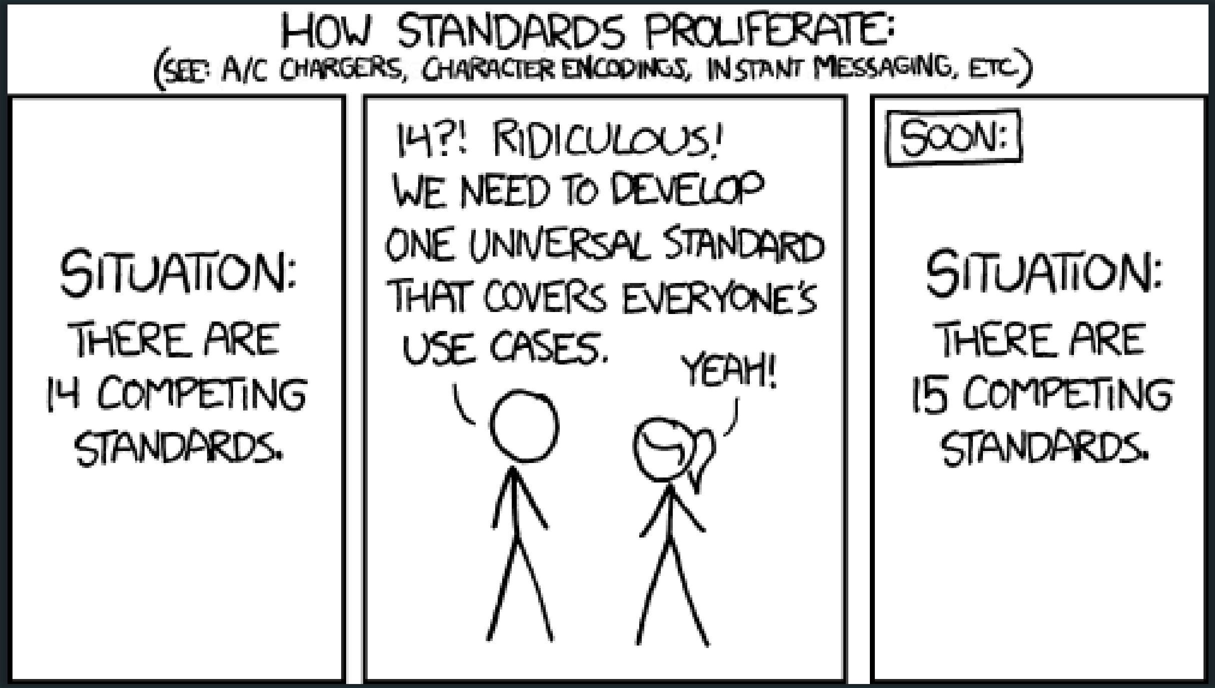

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Image from http://xkcd.com/927/

Simplicity vs. Complexity

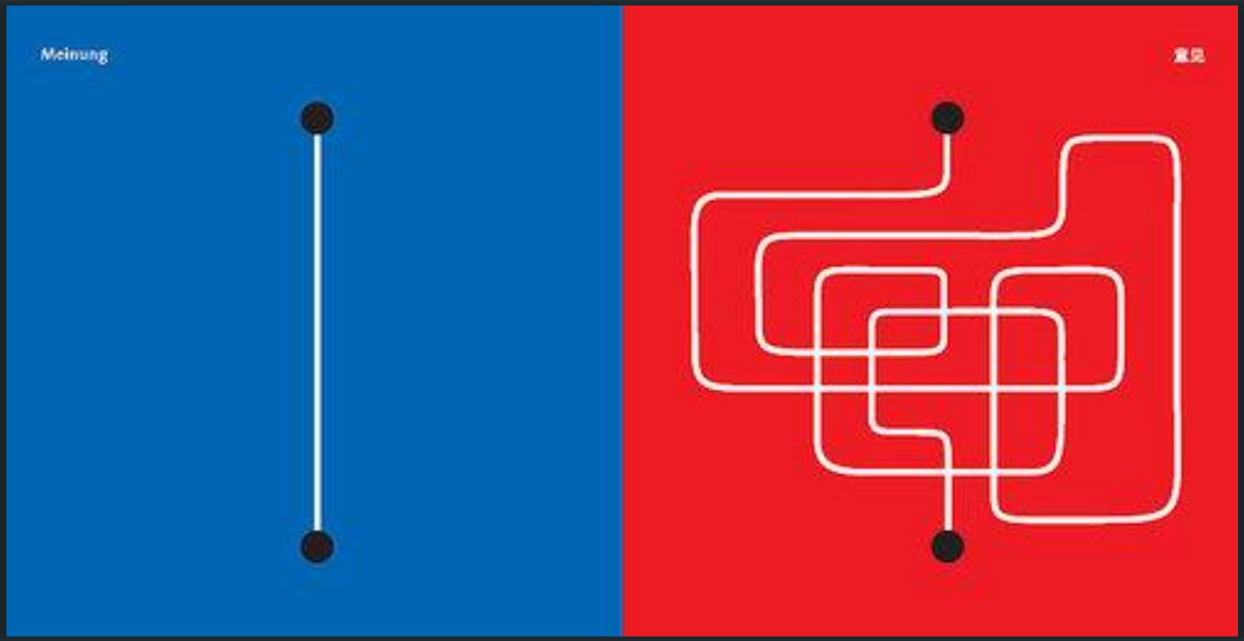


Image from http://www.brainpickings.org/wp-content/uploads/2009/10/eastwest_express.jpg

Try This On For Size

- 1 - Protect Your Applications
- 2 - Protect Your Endpoints
- 3 - Protect Your Network
- 4 - Protect Your Servers
- 5 - Protect Your Data
- 6 - Protect Your Locations
- 7 - Protect Your People

CSSF

Common Sense Security Framework

- This list isn’t in order of priority.
  - Priority will vary, depending on your organization’s risk appetite.

How Does It Work?

- Ask them 21 control questions
  - Yes or No answers
  - Let them explain to you how they enforce each control
- If they don't know how to implement a control, teach them!
  - Guidance
- Come back on a regular basis and ask them what's changed
  - In other words, update the spreadsheet
  - http://www.commonsenseframework.org/wp-content/uploads/2015/01/Common-Sense-Security-Framework-Questionnaire-v1.1.xlsx

1 – Protect Your Applications

- What’s in scope?
  - Web applications
  - Mobile applications
- How do we do it?
  - Teach your developers how to write secure code
    - Tons of free OWASP resources
  - Document your application security requirements
    - Project plans
    - Third party contracts
  - Scan your web applications for vulnerabilities

2 – Protect Your Endpoints

- What’s in scope?
  - Mobile devices (smartphones, tablets, laptops)
  - Workstations
  - Kiosks
  - Removable media

- How do we do it?
  - Install antimalware on <u>all</u> of your endpoints
  - Limit who has local admin rights
  - Patch all the things (operating systems + apps)

3 – Protect Your Network

- What’s in scope?
  - Wired network(s)
  - Wireless network(s)
  - Cloud network(s)
  - Remote access (VPN)
- How do we do it?
  - Segment your networks
    - Wired: regulated vs. corporate (vs. DMZ)
    - Wireless: corporate vs. guest (vs. BYOD, if you want to get fancy)
  - Use strong encryption for data in motion (internal and external)
  - Use multifactor authentication for remote access

4 – Protect Your Servers

- What’s in scope?
  - Directory servers (LDAP)
  - File servers
  - Web servers
  - App servers
  - Database servers
- How do we do it?
  - Harden your servers
  - Manage and monitor admin accounts (creation & usage)
  - Scan and patch your servers <u>on a regular basis</u>

5 – Protect Your Data

- What’s in scope?
  - Data at rest
  - Data in motion
- How do we do it?
  - Enforce the principle of least privilege via periodic user access reviews
  - Create (and test) backups of critical business data
  - Encrypt all of your restricted data at rest (i.e., stored on disk)

6 – Protect Your Locations

- What’s in scope?
  - Headquarters
  - Branch offices
  - Data centers
  - Retail outlets
- How do we do it?
  - Restrict access to sensitive locations and workspaces
  - Keep computing equipment (i.e., servers) in locked rooms
  - Require (or at the very least, encourage) employees to monitor visitors and challenge strangers

7 – Protect Your People

- What’s in scope?
  - Anyone who works for your company
  - Anyone who works with your company
- How do we do it?
  - Teach them how to identify and respond to potential security incident
  - Perform background checks as needed
    - What can they access?
    - Upon hire vs. recurring
  - Provide training on your internal policies, standards, and procedures
    - For the love of all things holy, folks, WRITE IT DOWN!

The End Result

- Simple question set
  - Short, sweet, and to the point
  - Accessible to both technical and non-technical people
- If they can’t answer yes to these 21 questions, then asking them anything else is a waste of everyone’s time
- IT’S NOT ABOUT COMPLIANCE!
  - It’s about helping the business owners understand the fundamentals of information security/technology risk management

Integrating the CSSF Into Your Business

- Step 1: Assess your current state.
- Step 2: Have an open, honest conversation about your risk appetite.
- Step 3: Set a goal for how secure you want to (or need to) be.
- Step 4: Determine how much money you’re going to spend each year on security.
- Step 5: Research solutions to help you meet your security goal within your security budget.
  - If a solution doesn’t exist in your price range, get creative!
- Step 6: Implement missing controls.
- Step 7: Schedule recurring tests to make sure your controls are working.
- Step 8: Measure the effectiveness of your controls.
  - Metrics, Dashboard, IT Risk Register, etc.
- Step 9: Repeat this process.

Resources

- Common Sense Framework
  - http://www.commonsenseframework.org/
- Information Security… Simplified
  - http://www.infosecsimplified.com/
- Information Security 101
  - http://slandail.net/
- IT Security Career
  - http://www.itsecuritycareer.com/

Resources

- OWASP Top Ten Project (Web)
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- OWASP Top Ten Project (Mobile)
  - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- OWASP Code Review Project
  - https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- OWASP Testing Project
  - https://www.owasp.org/index.php/OWASP_Testing_Project
- OWASP Vulnerability Scanning Tools
  - https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
- SANS SWAT Checklist
  - http://www.securingthehuman.org/developer/swat

Resources

- NIST SAMATE
  - http://samate.nist.gov/index.php/Tool_Survey.html
- SecTools.org
  - http://sectools.org/
- AV-Comparatives.org
  - http://www.av-comparatives.org/
- AV-Test.org
  - http://www.av-test.org/
- Center for Internet Security
  - http://www.cisecurity.org/
- SSL Labs
  - https://www.ssllabs.com/ssltest/

Summary

</rant>

Questions / Comments

?

Contact Info

Jerod Brennen, CISSP

CTO & Principal Security Consultant, Jacadis

LinkedIn: http://www.linkedin.com/in/slandail

Twitter: https://twitter.com/slandail

http://www.jacadis.com/

contact@jacadis.com