Securing the Supply Chain

Stuart Cianos, CISSP

scianos@alphavida.com

Disclaimer

The views and opinions expressed during this conference are those of the speakers and do not necessarily reflect the views and opinions held by the Information Systems Security Association (ISSA), the Silicon Valley ISSA, the San Francisco ISSA or the San Francisco Bay Area InfraGard Members Alliance (IMA). Neither ISSA, InfraGard, nor any of its chapters warrants the accuracy, timeliness or completeness of the information presented. Nothing in this conference should be construed as professional or legal advice or as creating a professional-customer or attorney-client relationship. If professional, legal, or other expert assistance is required, the services of a competent professional should be sought.

Securing the Supply Chain

Best Practices when Evaluating Third Party Technology Acquisition

3rd Party Software

- What is it?
  - Software that your organization did not author
    - Something you buy from another vendor for general use
      - ERP, CRM, even your word processor...
    - Open source software being implemented internally
    - A third party component or library being integrated into software authored by your organization
      - Your customers are running the software in their organization
  - Software that your organization may become responsible for via M&A, etc.
    - The third party software, and its dependencies and components, are about to be the responsibility of your organization.

3rd Party Software

- Why do we care?
  - The software is being used to support the business processes of the acquiring organization.
    - Customer information?
    - Employee information?
    - Proprietary business information and/or trade secrets?
    - Sensitive processes with revenue impact?
    - Sensitive processes with a life safety impact?
    - Reputation?
    - Potential liability?
    - Can it be used by an adversary to pivot on your network?
    - Who has access to the system and its data? (Feeling cloudy?)

3rd Party Software

- Why do we care?
  - The software is a component being integrated into software authored by your organization?
    - Your customer's:
      - Sensitive business information
      - Sensitive customer information
      - Proprietary business information and/or trade secrets?
    - Reputation?
    - Potential liability?
    - Is that component running in the same process space as other components in your system?
    - Can the component be used to further compromise the product's process space and/or gain lateral movement?

3rd Party Software

- Why do we care?
  - The product is being acquired by your company due to a merger and acquisition:
    - The acquiring organization is going to be responsible for the product and its ongoing maintenance/operation.
    - All of the bullet points noted on the previous slides, and more, may apply.
    - The acquiring organization may not have historical content.
    - The acquiring organization may not have accurate information on the progeny of the components which make up the system.
    - Analysis of the risk factors involved is very important.
      - What controls are in place?

Basic Processes...

- How do the right people know when 3rd party software is going to be acquired or integrated?

Basic Processes…

- How do the right people know when 3rd party software is going to be acquired or integrated?
  - No defined process or controls
  - Loose pre-acquisition management and/or technical controls (common in SMB)
  - Formal pre-acquisition controls (common in regulated and larger organizations)
  - Post-acquisition controls
- Political pain points

Basic Processes…

- How do the right people know when 3rd party software is going to be acquired or integrated?
  - No defined process or controls
    - Free for all. No standards.
    - No consistency among controls, review process, auditing.
    - Do you know what is actually in use? Inventory?
  - Loose pre-acquisition management and/or technical controls (common in SMB)
  - Formal pre-acquisition controls (common in regulated and larger organizations)
  - Post-acquisition controls

Basic Processes...

- How do the right people know when 3rd party software is going to be acquired or integrated?
  - No defined process or controls
  - Loose pre-acquisition management and/or technical controls (common in SMB)
    - May involve sending a request for authorization via COC
      - The Czar: Many times a manager in a small organization
    - Politically dangerous: may be hazardous to career in some orgs.
    - "One off" decisions and approvals
  - Formal pre-acquisition controls (common in regulated and larger organizations)
  - Post-acquisition controls

Basic Processes...

- How do the right people know when 3rd party software is going to be acquired or integrated?
  - No defined process or controls
  - Loose pre-acquisition management and/or technical controls (common in SMB)
  - Formal pre-acquisition controls (common in government, regulated and larger organizations)
    - The process is (hopefully) defined to avoid political runarounds and has formal controls which the business is in agreement with.
    - Multiple stakeholders typically involved, may require consensus.
    - Usually distributes accountability amongst multiple stakeholders.
  - Post-acquisition controls

Basic Processes…

- How do the right people know when 3rd party software is going to be acquired or integrated?
  - No defined process or controls
  - Loose pre-acquisition management and/or technical controls (common in SMB)
  - Formal pre-acquisition controls (common in government, regulated and larger organizations)
  - Post-acquisition controls
    - Acquisition may be discovered during change control process, or as a request to implement the system.
    - Likely already made an investment in the system. Provides political fodder to implement absent controls or review.

On Premise vs. Cloud

- Doesn't matter: Consider all insecure by default
  - Apply review and control protocols to both on-premise and "cloud" systems.
  - A cloud system can be used to pivot into an on-premise network:
    - SSRF, CSRF, IDOR, XSS and more.
    - Users tend to trust their own systems.
    - Example: Compromised "cloud" web application vulnerable to XSS is used to initiate external contact (in the context of the user).
  - A vulnerability on your network can pivot into cloud apps.
  - Boundaries are no longer as clear as they used to be…
  - Probably additional controls specific to each.

We've covered the basics...

- Let's talk about assessment…
  - What drives the requirements of your organization?
    - Regulatory compliance
    - Licensing requirements
    - Technical requirements
    - Business requirements
  - Assessing the software (and vendor)
    - Regulatory compliance
      - Business associate agreements, certifications, reg. approvals, etc.
    - Licensing requirements
      - In general: Are the terms acceptable? Do they pass legal?
      - As a component: Is the component distributable/allowed for your use case?
      - For open source components, some organizations are adverse to "viral" licenses. Know how the component will be linked, and how that impacts your use of the component.

Tools of the Trade:

- Assessing the software & vendor
  - Self-Assessment
  - Demonstration
  - Technical Review and/or Audit (including dependencies!)
  - Legal Review of Contract and Licensing Terms
  - Business Process and Regulatory Compliance Audits
  - Financials Review
  - Operational Practices (significant security impact!)
- Spice up your assessments
  - New tools are becoming available to make your job easier
    - VSAQ: interactive questionnaire application to assess the security programs of third parties… https://github.com/google/vsaq

"Shrink-Wraps"

- A term I'm using to loosely group together both on-premise and internet-delivered (ASP) applications.
  - Reality check…
    - Intuit probably isn't going to negotiate with your small business over a licence for QuickBooks.
    - Microsoft probably won't complete a self-assessment questionnaire when you purchase a 5-pack of Microsoft Office.
    - Off-the-shelf software typically has standard T&C's and licensing.
    - Delivery of end-user applications across the internet via application service providers has become normalized.
    - The ease of end-user implementation of zero-install applications can result in unexpected consequences if processes, policies, and other controls are not in place.

Tools of the Trade:

- More limited menu for "Shrink-Wraps":
  - Self-Assessment
  - Demonstration
  - Technical Review and/or Audit (including dependencies!)
  - Legal Review of Contract and Licensing Terms
  - Business Process and Regulatory Compliance Audits (i.e. PCI)
  - Financials Review
  - Operational Practices (significant security impact!)
- You will likely be performing all of the above assessments using your own resources for off-the-shelf products.

Self-Assessment: Thoughts...

- Technical
  - Technical standards and dependencies
  - Operational standards and practices
  - Information Security (C.I.A.):
    - Design: The product's design and implementation is secure.
    - Posture: The product **and its supporting infrastructure and dependencies** are aggressively maintained to meet the confidentiality, integrity, and availability requirements of your organization. Also see operational standards...
    - Capability: The product has the ability to meet your general information security requirements and policies.
    - Physical: For products which host data off-premise, what are the physical security protocols in place to protect sensitive data?

Self-Assessment: Thoughts…

- Technical
  - Technical standards and dependencies
    - Hardware requirements
    - Operating system requirements/preferences
    - Database platform dependencies
    - Many other dependencies: Java, .NET?
      - The vendor should identify their dependencies!
    - Network infrastructure requirements
    - Browser requirements and minimum/maximum versions
  - Know the requirements necessary to support the application to determine if it will easily integrate into your environment.
  - Are you able to support and maintain the application?

Self-Assessment: Thoughts…

- Technical
  - Technical standards and dependencies
  - Operational standards and practices
    - What is the service level agreement for the application?
      - How does the vendor meet the terms of the SLA?
      - BC/DR technical processes and controls?
    - How is the application source maintained and audited?
      - Source revision control? Waterfall? Agile? CI/CD? TDD?
    - How is infrastructure maintained and audited (ASP)?
      - Configuration management?
      - Source revision control on CM code/configs?
      - Is this an "artisan" network?
    - How is the software tested before release to the customer?
    - Staff/developer training re: Security… The human element?

Self-Assessment: Thoughts...

- Technical
  - Technical standards and dependencies
  - Operational standards and practices
  - Information Security (C.I.A.):
    - Design: The product's design and implementation is secure.
    - Posture: The product **and its supporting infrastructure and dependencies** are aggressively maintained to meet the confidentiality, integrity, and availability requirements of your organization. Also see operational standards...
    - Capability: The product has the ability to meet your general information security requirements and policies.
    - Physical: For products which host data off-premise, what are the physical security protocols in place to protect sensitive data?

Self-Assessment: Thoughts...

- Technical
  - Technical standards and dependencies
  - Operational standards and practices
  - Information Security (C.I.A.):
    - Design: Fatal flaws...
      - If the product is a client/server-based application, does the client directly connect to the back-end database (i.e. 2 tiers)?
        - How is the database secured against a client-side attack? Stored procedures? Table, row, or cell level permissions?
      - If the product is presented through a web browser, how does the application's ***framework*** protect against web-borne attacks such as those described in the OWASP TOP 10?
        - Just because it's accessed internally doesn't mean it's not a risk.

Self-Assessment: Thoughts...

- Technical
  - Technical standards and dependencies
  - Operational standards and practices
  - Information Security (C.I.A.):
    - Design: Fatal flaws...
    - Posture: The operational side of C.I.A.
      - How is the system monitored for security and operational events?
        - Service Monitoring? Metrics? Traffic analysis? IDS? Logs? SIEM?
      - How are technical controls layered to avoid lateral movement and pivoting in the event of a failure or breach?
      - How are components and systems monitored for known and unknown (zero-day) security vulnerabilities? *Pen-testing?*
      - How is information protected or encrypted in transit and at rest?
      - How does the system guarantee the integrity of a transaction?

Self-Assessment: Thoughts…

- Technical
  - Technical standards and dependencies
  - Operational standards and practices
  - Information Security (C.I.A.):
    - Design: The product's design and implementation is secure.
    - Posture: The operational side of C.I.A.
    - Capability: Integration with your controls
      - Can the product be configured securely? There are cases of software which has a secure design but lacks features necessary to securely configure it.
        - Does the application integrate with enterprise directories or SSO solutions? How?
        - Can basic controls like password complexity, timeouts, and maximum attempts be configured?

Self-Assessment: Thoughts…

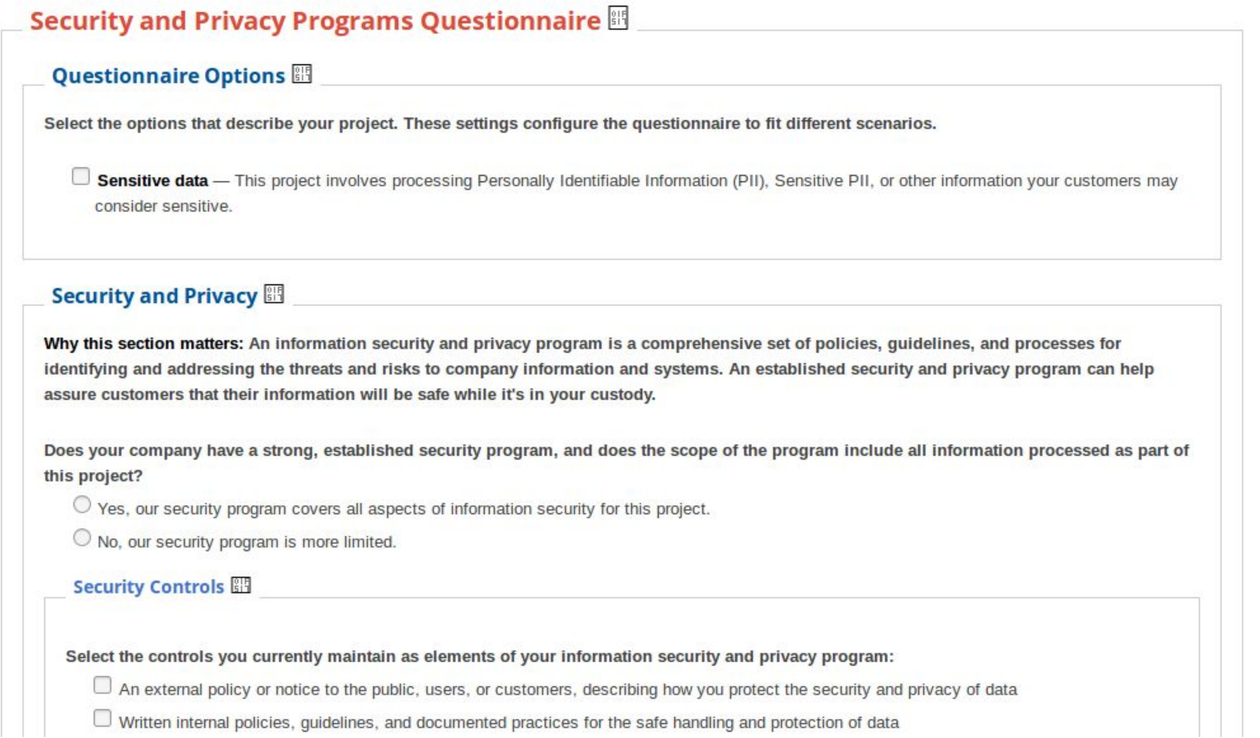
- Technical
  - Technical standards and dependencies
  - Operational standards and practices
  - Information Security (C.I.A.):
    - Design: The product's design and implementation is secure.
    - Posture: The operational side of C.I.A.
    - Capability: Integration with your controls
    - Physical: Is the door open?
      - Have background checks been performed on staff with access?
      - How is the data and systems physically secured? DC security protocols? 2FA? What DC and where?
      - Equipment DR protocols? Asset inventory audits?

Resources for Assessments:

- Traditional tools:
  - NIST Special Publication 800-53: A comprehensive catalog of security and privacy controls for federal information systems. Useful for any organization looking for a comprehensive catalog to select from.
    http://csrc.nist.gov/groups/SMA/fisma/assessment.html
    https://web.nvd.nist.gov/view/800-53/home
  - NIST Cybersecurity Framework
    http://www.nist.gov/cyberframework/
  - ISO 27001
- New tool:
  - VSAQ: interactive questionnaire application to assess the security programs of third parties… https://github.com/google/vsaq

A quick look at VSAQ:

- A software framework which may be used to provide an electronic self-assessment questionnaire:



Security and Privacy Programs Questionnaire

Questionnaire Options

Select the options that describe your project. These settings configure the questionnaire to fit different scenarios.

□ **Sensitive data** — This project involves processing Personally Identifiable Information (PII), Sensitive PII, or other information your customers may consider sensitive.

Security and Privacy

Why this section matters: An information security and privacy program is a comprehensive set of policies, guidelines, and processes for identifying and addressing the threats and risks to company information and systems. An established security and privacy program can help assure customers that their information will be safe while it's in your custody.

Does your company have a strong, established security program, and does the scope of the program include all information processed as part of this project?

○ Yes, our security program covers all aspects of information security for this project.

○ No, our security program is more limited.

Security Controls

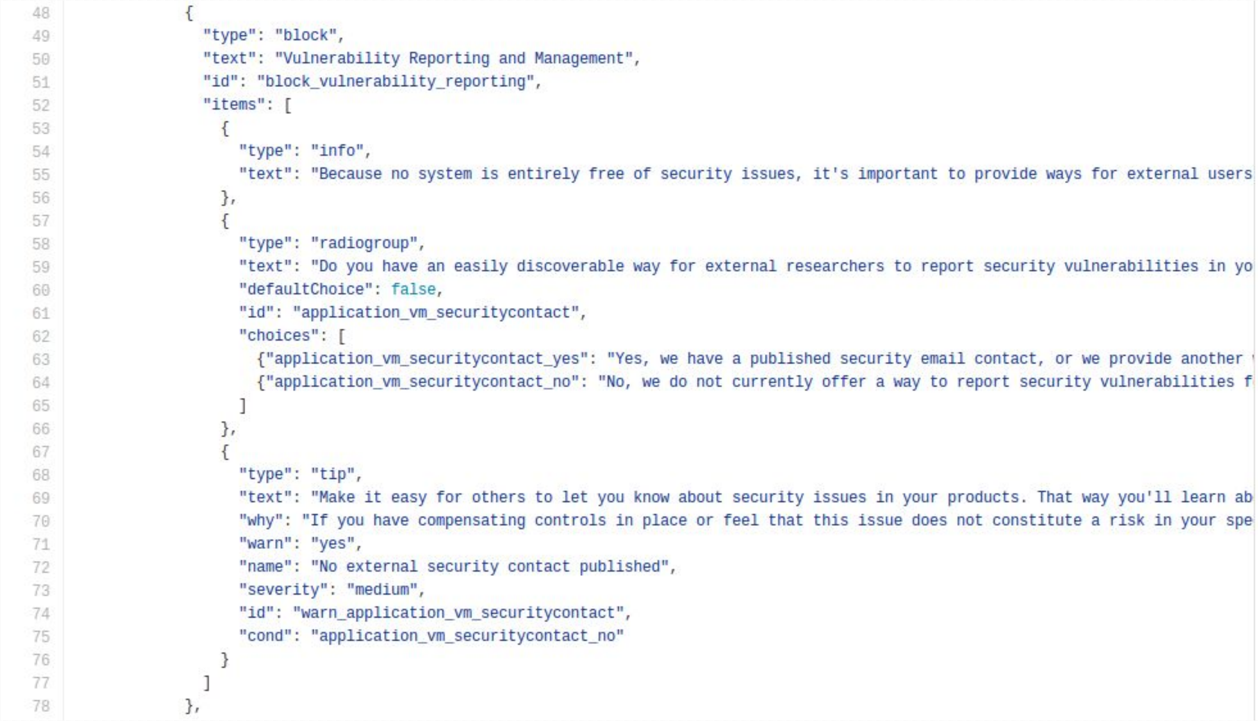
Select the controls you currently maintain as elements of your information security and privacy program:

□ An external policy or notice to the public, users, or customers, describing how you protect the security and privacy of data

□ Written internal policies, guidelines, and documented practices for the safe handling and protection of data

A quick look at VSAQ:

- A software framework which may be used to provide an electronic self-assessment questionnaire.
- A *very* useful source of controls in a structured format:



```
{
  "type": "block",
  "text": "Vulnerability Reporting and Management",
  "id": "block_vulnerability_reporting",
  "items": [
    {
      "type": "info",
      "text": "Because no system is entirely free of security issues, it's important to provide ways for external users
    },
    {
      "type": "radiogroup",
      "text": "Do you have an easily discoverable way for external researchers to report security vulnerabilities in yo
      "defaultChoice": false,
      "id": "application_vm_securitycontact",
      "choices": [
        {"application_vm_securitycontact_yes": "Yes, we have a published security email contact, or we provide another
        {"application_vm_securitycontact_no": "No, we do not currently offer a way to report security vulnerabilities f
      ]
    },
    {
      "type": "tip",
      "text": "Make it easy for others to let you know about security issues in your products. That way you'll learn ab
      "why": "If you have compensating controls in place or feel that this issue does not constitute a risk in your spe
      "warn": "yes",
      "name": "No external security contact published",
      "severity": "medium",
      "id": "warn_application_vm_securitycontact",
      "cond": "application_vm_securitycontact_no"
    }
  ]
},
```

A quick look at VSAQ:

- A software framework which may be used to provide an electronic self-assessment questionnaire.
- A *very* useful source of controls in a structured format:
  - Infrastructure
  - Physical Security
  - Data Center Security
  - Privacy
  - Web Application Security

Back to the Tools of the Trade…

- Still a couple of points to touch upon:
  - Self-Assessment
  - Demonstration
  - Technical Review and/or Audit (including dependencies!)
  - Legal Review of Contract and Licensing Terms
  - Business Process and Regulatory Compliance Audits
  - Financials Review
  - Operational Practices (significant security impact!)
- We'll make it quick!

Back to the Tools of the Trade…

- Still a couple of points to touch upon:
  - Demonstration
    - Demonstrate the functionality of the system, hands-on (both its intended purpose and security features)
      - True stories from the 9th circle: A vendor traveled cross country to propose the implementation of a system with a life safety critical element. When asked to demonstrate the product, the vendor presented screenshots in a presentation. When asked to demonstrate a running instance of the software, the potential customer learned that it had not been developed sufficiently for production use. The screenshots were a mock-up.
    - If permissible and with the contracted/written permission of the vendor, consider periodic coordinated penetration testing.

Back to the Tools of the Trade…

- Still a couple of points to touch upon:
  - Demonstration
  - Legal Review of Contract and Licensing Terms
    - Counsel should be involved in a review of the T&C's, licensing.
    - Helpful during negotiations, if they are taking place.
    - Ensure regulatory requirements are covered in the agreement as necessary:
      - Business associate agreements
      - Compliance reporting requirements for PCI
      - Ability to test and audit the vendor's systems as necessary
      - If the product is not open source and/or the source code is not included with the product, source escrow may be useful.
        - May also be useless if you don't know how to compile and maintain the application.

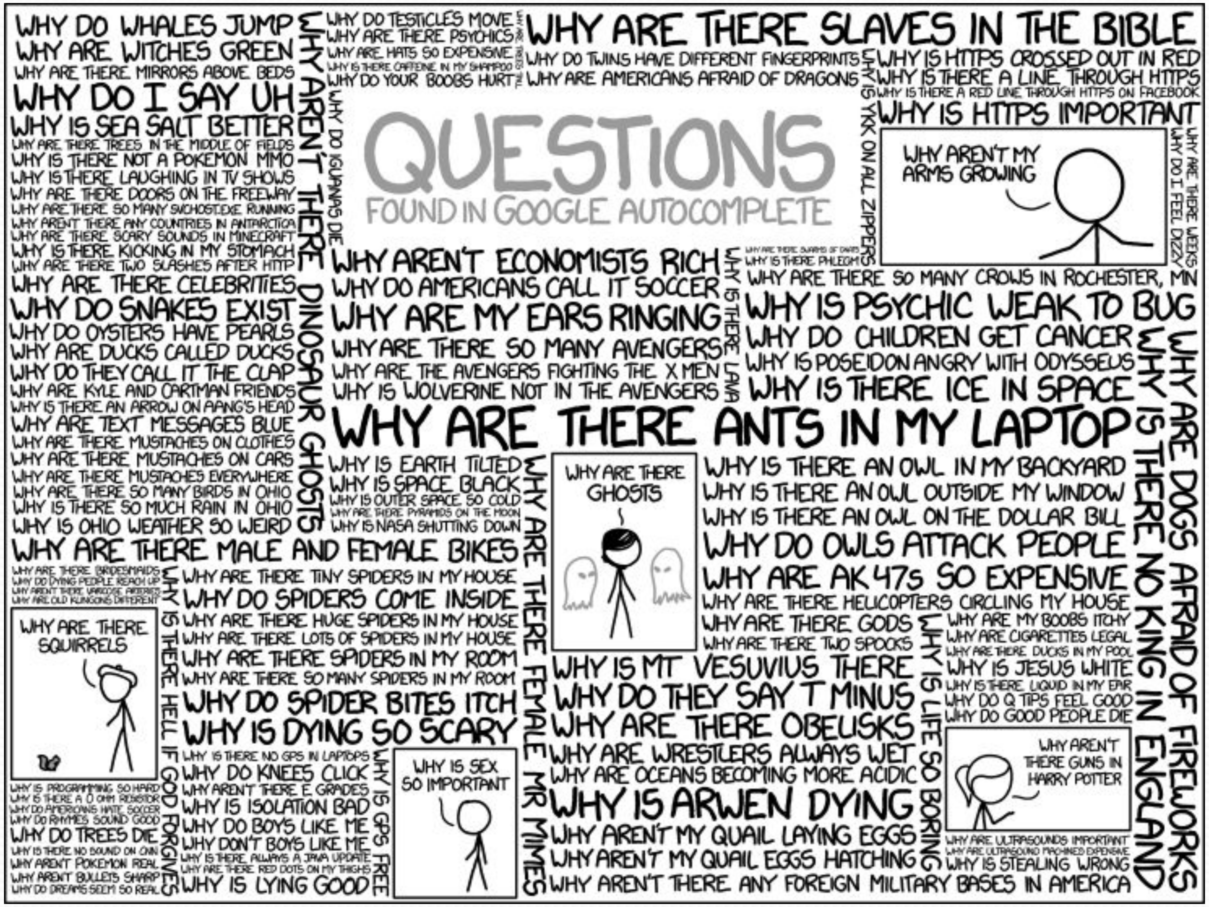
Back to the Tools of the Trade…

- Still a couple of points to touch upon:
  - Demonstration
  - Legal Review of Contract and Licensing Terms
  - Business Process and Regulatory Compliance Audits
    - Is the vendor able to provide PCI auditing certificates? QSA?
    - Compliance with breach notification reporting?
      - If the vendor has PII, how do they report incidents?
        - Can you meet ***your*** regulatory requirements to ***your*** customers based on the contracted obligations of the vendor?
    - Does the vendor purport ISO 27001 compliance, or compliance with any other myriad of security control frameworks?
    - COSO? COBIT? ISO? ITIL? BITS? SAS 70?

Back to the Tools of the Trade…

- Still a couple of points to touch upon:
  - Demonstration
  - Legal Review of Contract and Licensing Terms
  - Business Process and Regulatory Compliance Audits
  - Financials Review
    - Typical only when assessing high cost acquisitions, and/or those software acquisitions which would have a major impact on business operations should the vendor cease operation.
    - May provide useful indicators of the vendor's business health and outlook
    - Considered confidential by most firms. Usually requires an NDA.
    - Assess the risks around the vendor's solvency.

Questions?


QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY AREN'T THERE DINOSAUR GHOSTS
WHY DO IGUANAS DIE
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY ARE TREES TALL
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS YKK ON ALL ZIPPERS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY AREN'T MY ARMS GROWING
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY ARE THERE SWARMS OF GNATS
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOCKS
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY IS THERE NO KING IN ENGLAND
WHY ARE DOGS AFRAID OF FIREWORKS
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE OLD KLINGONS DIFFERENT
WHY ARE THERE SQUIRRELS
WHY IS THERE HELL IF GOD FORGIVES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS SEX SO IMPORTANT
WHY ARE THERE FEMALE MR MIMES
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY IS LIFE SO BORING
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG

https://xkcd.com/1256/

Thank you

Stuart Cianos

scianos@alphavida.com

Disclaimer

The views and opinions expressed during this conference are those of the speakers and do not necessarily reflect the views and opinions held by the Information Systems Security Association (ISSA), the Silicon Valley ISSA, the San Francisco ISSA or the San Francisco Bay Area InfraGard Members Alliance (IMA). Neither ISSA, InfraGard, nor any of its chapters warrants the accuracy, timeliness or completeness of the information presented. Nothing in this conference should be construed as professional or legal advice or as creating a professional-customer or attorney-client relationship. If professional, legal, or other expert assistance is required, the services of a competent professional should be sought.