Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

June 5, 2019

ISOAG June 5, 2019 Agenda

I. Welcome and Opening Remarks	Mike Watson, VITA
II. Managing Security from a Legal Perspective	Beth Burgin Waller, Esq.
III. Archer Update	Mark Martens, VITA
IV. Vulnerability Scanning Update	Bill Freda, VITA
V. ATOS ISO Update	Kathy Bortle, VITA Darrell Raymond, ATOS
VI. Upcoming Events	Mike Watson, VITA

Managing Security Risk From a Legal Perspective: 15 Tips

1

Where do legal risk and cyber risk intersect?

125 YEARS

- Cyber risk often intersects with legal risk:
  - Data breach / notification
  - Breach of contract
  - Loss of trust
  - Media frenzy

2

Third party vendors and assessments

125 YEARS

- Assessments, SOC 2s, and security questionnaires are important tools.
  - But are you **relying on someone else's self assessment or attestation**?
  - If a security questionnaire – do you have an "oath" page of sorts?
  - SOC 2 has its own problems legally
- Outsourcing the review?

3

Document, document, document

125 YEARS

- Get it in writing every time and keep records of what was represented to you about their services and security.
- Wheever possible – send a confirmation email of what is represented to you on the phone about a service or application, especially if it is a critical platform or tool.

4

Contract basics

125 YEARS

- Offer + Acceptance = binding contract!
- Contracts **do not** have to be physically signed to be binding.
- Under certain circumstances, email correspondence can be used against you to evidence the existence of a contract **even without a signed document**.

5

Breach notifications

125 YEARS

8. **BREACH NOTIFICATION**

8.1 In respect of any actual Protected Data Breach, the Data Processor shall, as soon as reasonably practicable:

8.1.1 notify the Data Controller of the Protected Data Breach; and

8.1.2 provide the Data Controller with details of the Protected Data Breach.

9. **DELETION OR RETURN OF PROTECTED DATA AND COPIES**

9.1 The Data Processor shall delete or return all the Protected Data in its possession to the Data Controller in accordance with the terms of the Agreement unless prohibited by Applicable Law.

What does “as soon as reasonably practical” mean and if you needed to know about a breach, would you want to find out?

6

Return of data

125 YEARS

DELETION OR RETURN OF PROTECTED DATA AND COPIES

9.1 The Data Processor shall delete or return all the Protected Data in its possession to the Data Controller in accordance with the terms of the Agreement unless prohibited by Applicable Law.

If we share information with them, how are we getting it back?

7

Termination aka “how do we get out of this mess?”

125 YEARS

8. TERM AND TERMINATION

8.1 Each Complete Agreement shall commence on the Effective Date stated on the applicable Order Form and shall continue for the period of the Term specified on that Order Form and:

(a) if renewed in accordance with a provision of that Order Form, for the applicable renewal period; and

(b) if there are [redacted] Periods still running, until the end of the all those [redacted] Periods, unless terminated earlier in accordance with the terms of the Complete Agreement.

8.2 Either party may, upon giving written notice to the other, suspend performance of and/or terminate a Complete Agreement with immediate effect if:

(a) the other party is in material breach of that Complete Agreement and such breach is incapable of remedy; or

(b) the other party is in breach of that Complete Agreement and, where such breach is capable of remedy, fails to remedy such breach within 30 days of being so requested; or

Where possible, do not agree to only a “termination for cause” type provision.

8

Indemnification

125 YEARS

- Indemnification is the ability to seek reimbursement for losses/expenses/legal fees from another party.
- Depending on the contract language, can be from the opposing party or another third party.

9

Watch terms that move…

125 YEARS

Except as the parties expressly agree otherwise, these Terms constitute the entire agreement between the parties relating to the subject matter hereof and supersede all prior understandings, writings, proposals, representations or communications, oral or written, of either party. These Terms may only be amended by an instrument executed by the authorized representatives of both parties.

"Privacy Notice"	Means Provider's EU Privacy Policy as such appears on its website and as is attached to this Schedule 1 as Exhibit A. Notice of any changes to

10

The information security agreement

125 YEARS

The Provider wishes to provide certain services to ("**Services**") pursuant to the service agreement between the parties ("**Service Agreement**"). The purpose of this ISA is to establish the minimal electronic and physical information security measures and requirements in relation to how Data (as defined below) is stored, accessed, used or otherwise processed by the Provider in connection with the Services. Security requirements in this ISA must be followed always, including in the event of a disaster or force majeure event. To the extent of any inconsistencies or conflict, this ISA takes precedence over the Service Agreement in relation to its subject matter.

11

More about the ISA

125 YEARS

10.1. Access [redacted] networks and WestRock Data only through an approved secured connection.

10.2. Multi-factor authentication must be used for any remote access.

10.3. No dial-up connection may be used to connect to the [redacted] network or to connect to Provider's network to access WestRock Data unless provider receives WestRock's written permission.

10.4. Wireless access points must be appropriately secured.

10.5. Only Authorized Personnel may use the User ID and password provided to access [redacted] networks. Shared accounts or system accounts are not permitted for access.

10.6. Devices with access to [redacted] Data must be locked while unattended.

10.7. All software on equipment used to store, access, use or otherwise process [redacted] Data must be properly licensed.

10.8. Only an authorized device (e.g., desktop, laptop, smart phone, tablet, etc.) may be used to store, access, use or otherwise process or connect to WestRock Data with the following measures in place (each an "**Authorized Device**"):

(a) appropriate access controls including, a User ID and password;
(b) ability to lock device to restrict access;
(c) timeout and lock after a maximum of 15 minutes of inactivity;
(d) anti-virus, anti-malware software with a mechanism for regular updates;
(e) secure configuration;
(f) patch management to keep the software up to date;
(g) restricted or disabled transfer of data to portable storage mediums without permission;
(h) Encryption of data on portable devices;
(i) remote wiping for portable devices when lost or stolen; and
(j) any other measures required in order to comply with this ISA.

10.9. All reasonable precautions must be made to ensure viruses are not transferred to [redacted] systems through a connection.

10.10. Token based authentication or another restricted VPN access must be used if requested by [redacted]

10.11. Software which is considered or suspected to pose a security risk or legal concern to [redacted] Data o[redacted] must be removed from Provider devices upon request.

12

Re-assess

125 YEARS

- It’s not sufficient that they once passed the test five years ago - each renewal the same level of review must be used.

13

Document the problems

125 YEARS

- If you have a problem with a service or solution, make sure you are setting up a breach scenario the right way by writing about the issues to the third-party service provider.

14

When to call the lawyers

125 YEARS

- Confidentiality and privilege only work if you get an attorney involved early in a dispute scenario.

15

What does their insurance say?

- Great to have cyber insurance obligations, but do you know what insurance they actually have?
- Does it only cover first party versus third-party breach?

Beth Burgin Waller

bwaller@woodsrogers.com

125 YEARS

Virginia Information Technologies Agency

Web Application Vulnerability Scanning Update

VITA
Commonwealth Security and Risk Management

June 5, 2019

COV web application vulnerability scanning program

- History
  - 2009 incident scans to paid service to legislative support for all systems in FY17. Running for almost three years
- Status
  - 98% compliance, continued reduction in critical vulnerabilities, footprint reduction, partnering with agencies to reduce risks. You receive quarterly scans and reports
- Future
  - Integrating internal sensitive applications into the program, further reduction. Vulnerable, high-risk applications apparent
- How you can help
  - Review reports and remediate, ask for assistance if needed

Results and Archer

- High and medium alerts in Archer
  - Cleanup process – thank you! 23,600 to 7,000 with 4,000 of those closed.
  - Volume is overwhelming at about 72,000 alerts per quarter
- Agency role
  - Ensure each scan has a matching application
  - Review repeat high and medium findings
  - Become familiar with this in Archer. Once we have our part set, agencies will be tasked with updating these in Archer.

Archer - application

Please make sure applications with URLs have them listed

Alert trends and alert reduction

- We scan 1,500 unique URLs per quarter
  - Alerts are being remediated across the board
  - Average days to remediate alerts
  - The trend appears to be leveling out
  - Repeat high and medium alerts are visible

- ISO role – Guide application developers and webmasters to strive for a culture that creates secure, resilient applications to reduce alerts

Quick response to critical alerts

- Generally, agencies respond quickly when we let you know about open high-risk alerts
- Typically we have notified agencies prior to the incident
- Running known vulnerable software is the number one risk
- Know what version you are running and when security updates are released

How can we improve

- Do not roll out new sites or overhauled sites without pre-release scans
- Let us know about new sites, governance and scanning
- Add private, sensitive sites, dev and pre-release scans to the program
- Reporting process changes
- Acu-sensor
- Your program. What would make it better?

Summary

- Work on URL designations for applications
- Keep Archer current
- Read your quarterly reports. Test and remediate vulnerabilities. Review each alert. Ask for help.
- Try to reduce the average days to close alerts
- Know what version software is running and be aware of security updates

Questions?

Virginia Information Technologies Agency

Archer Updates

Presenter
Mark Martens

ISOAG
June 5, 2019

Assurance model

- Products and services
  - System security plans
  - Service tower applications
    - You will have your own instance as they go into production this summer
  - Business processes and data sets
    - You will be given generic ones and need to customize them to fit how your organization uses these services
    - Audits and risk assessments
      - Service towers are contractually required to provide SOC audits, ISO 27001 audits
      - Results of those audits will be provided to you

Assurance model

- What?!?

For every enterprise application, you will receive an instance in your inventory. This allows you to review the system security plans, audits, risk assessments, and findings associated with this application. Just like any other application that your organization utilizes, you are required to assess the way that you use the application and what kind of data you put in that application and what risks are associated with the way your organization uses it. We have started you off with a generic business process and data set. We will also map it to the appropriate devices as we receive that information. Expect many more to come.

Navigate to products and services

- In Archer go to:
- Agency workspace
  - Business infrastructure
    - Products and services

Enterprise products and services

- Current applications:
  - G Suite
  - Help desk
  - Mainframe
- Future applications:
  - New services
  - Agency provided services like Cardinal, PMIS
  - Example: Cardinal VITA

Risk assessment questionnaire

- Beta mode
  - Our centralized ISO services have begun using the questionnaire
  - We have received input on ways to improve the questionnaire
    - Allow for selection of questions by assessor
    - Include more technical questions
    - Add helper fields that provide test steps
    - Create comments and name fields that will populate subsequent findings

MSS new required services and team introduction

Virginia Information Technologies Agency

Incident Response Process

Kathy Bortle, CISSP, GCIH, GCIA, GPEN, GWAPT, GMOB, PMP

Commonwealth Security and Risk Management
Incident Response Specialist

ISOAG

June 5, 2019

Roles in new world

- CSRM – liaison with the agency, the MSI and the MSS
- MSS - owns the incident ticket
- MSI - coordinates getting what ATOS

FIAR forms

- FAIR forms are required for anything that the agency can't pull for themselves
- VCCC has been instructed to request a FIAR and assign the ticket to CSRM incident response
- CSRM determines if a FIAR is required and requests the form if appropriate
- CSRM forwards the ticket to the SOC for processing

ISO knowledge sharing site

Link:
https://covgov.sharepoint.com/sites/VITASec/ISOKnowledgeSharing/SitePages/Home.aspx

- Discussion forum
- Archer training materials

MSS New Required Services and Team Introduction

Presenter
Presenter Title

ISO AG
June 5th, 2019

Agenda

- MSS new required services
  - Network compliance
  - Enterprise data encryption
  - Certificate management
  - Server host intrusion detection and prevention system (HIDS/HIPS)
- MSS team introduction

Network Compliance

Overview – Network compliance

Network compliance monitors the network infrastructure to discover devices as they connect to the network.

Allows VITA and agencies to set policies that establish the specific behaviors the device can have while connected to a network.

Enterprise Data Encryption Services

Overview – enterprise data encryption services

- Default option - tokenization
- Protect file - server and application file/folder level encryption
- Protect app – application level encryption
- Database native - native database encryption connector
- KMIP connector - encryption connectors
- ProtectV – virtual machine encryption
- ProtectDB - column-level database encryption and protection

Certificate Management

Overview – certificate management

Certificate management service will provide a multi-tenant suite of certificate management for servers and end-user devices. The service automates and validates the entire issuance and renewal process.

- Enforces VITA's standard certificate requirements and identifies invalid certificates
- Provides controls that prevent certificate-based outages
- Enables self-service credential management through a web-based, policy enforced, self-service portal

Server Host Intrusion Detection and Prevention System (HIDS/HIPS)

Overview – HIDS/HIPS

- Advanced threat protection through our dynamic, stateful host firewall
- Installation, update, upgrade, patch, operation and maintenance of the HIPS in accordance with security requirements and VITA rules
- Integration with McAfee's global threat intelligence (McAfee GTI) network connection reputation to secure hosts against advanced threats such as botnets, distributed denial-of-service (DDoS), and emerging malicious traffic before attacks can occur

MSS Team Introduction

Atos team

Information Systems Security Officer

Chris Schurman

Chief Operations Manager

Jeff Lamons

Business Relationship Manager

George Cosby

Service Delivery Manager

Darrell Raymond

Upcoming Events

Future ISOAG

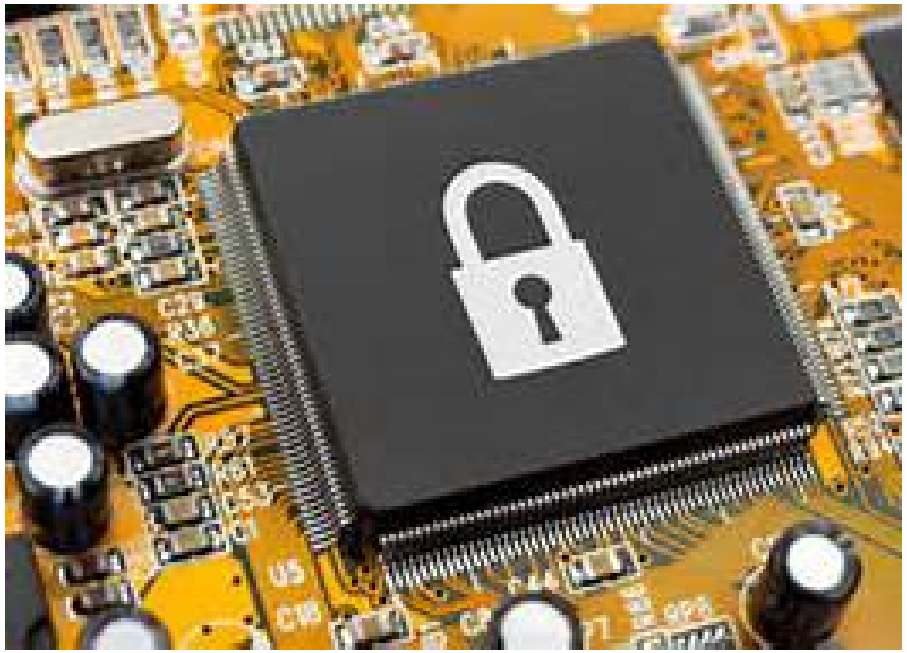
July 10, 2019 at CESC 1-4 p.m.

Speakers: David Ihrie, CIT
John Chiedo, Chiedo Labs
Chad Owens, LVA

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING



Picture courtesy of www.v3.co.uk