RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-T09

DUE DILIGENCE MEETS SMALL BUSINESS: NIGHTMARES FROM THE OTHER SIDE

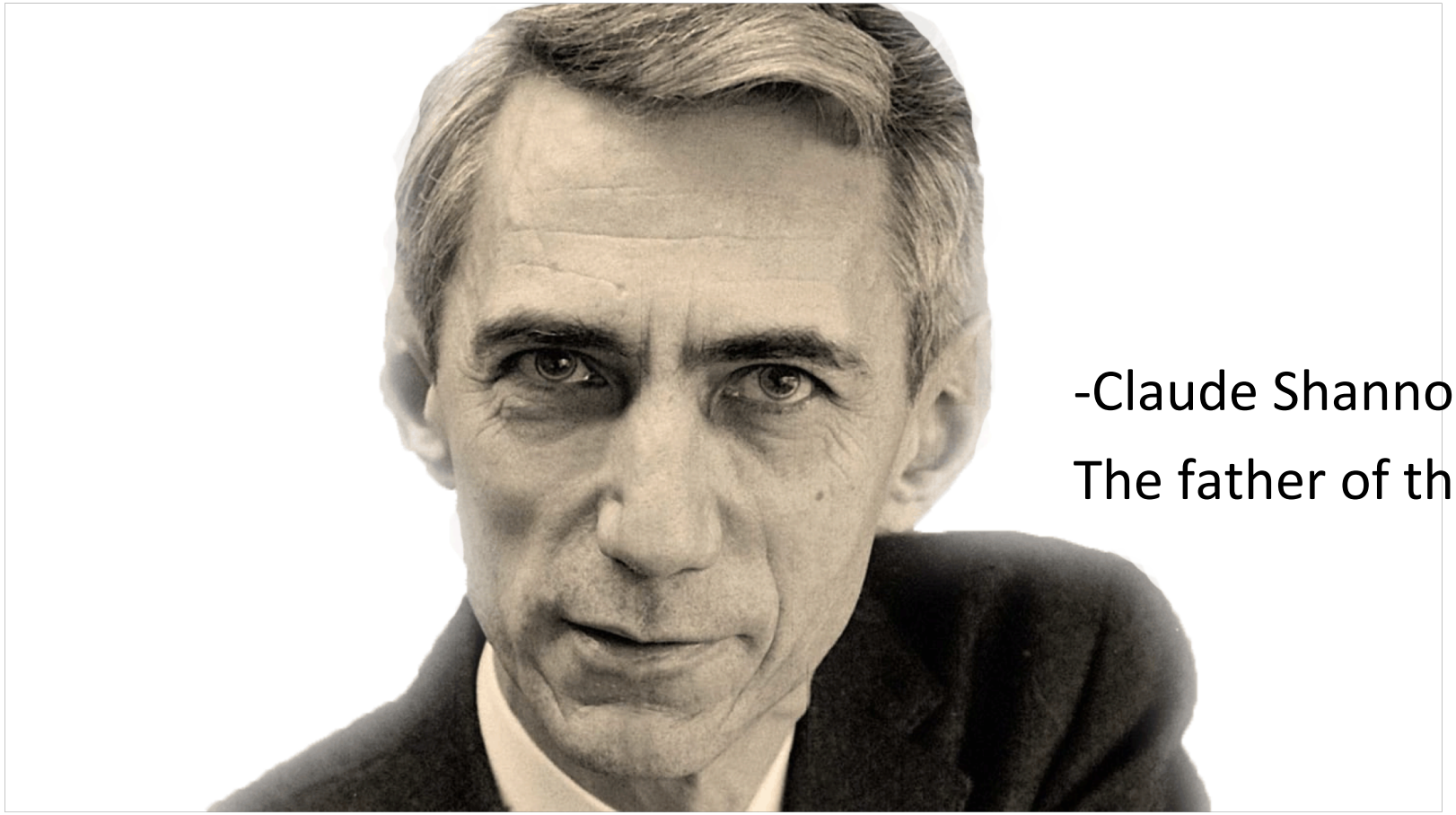
LAWRENCE CRUCIANA

CHIEF SYSTEMS ENGINEER
CORPORATE INFORMATION TECHNOLOGIES

@lcruciana

INTRODUCTION

"Information is the resolution of uncertainty"



-Claude Shannon

The father of the information age

AGENDA

- Understanding the landscape
- Looking at both sides: 3 case studies
- Effective tools & techniques
- Applying these lessons
- Tools & References (for later use)

Attendee Poll

- SESSION: PDAC-T09

How large is your organization?

1-100 Employees

101-499 Employees

500+ Employees

https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3848

The Landscape

- Small businesses is Big!
- ~97% of all employers are Small Businesses[1,2]
  - 5-99 Employees
  - <$11M Total Revenue
  - Single location

1 US Census Bureau; https://www.census.gov/programs-surveys/ase/data/tables.html Retrieved 1/25/19
2 Small Businesses <$11M revenue and 5-99 Employees, sbecouncil.org Retrieved December 2, 2018

The Landscape

- SO WHAT?!
- Most enterprises have >600 Suppliers [2]
- Small and Medium Businesses (SMB) represent up to 65% of suppliers[1]

1 CAPS Research; Business Partner Engagement Report
https://www.capsresearch.org/

2 Forbes, Feb 2018
https://www.forbes.com/sites/jwebb/2018/02/28/how-many-suppliers-do-businesses-have-how-many-should-they-have/#5276f4ea9bb7

The Landscape

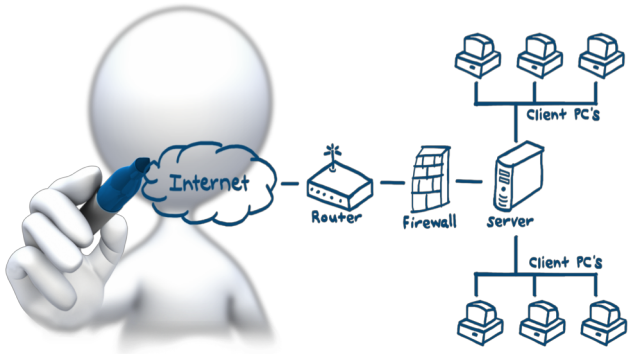
- Small businesses are largely not equipped to measure risk
- Few (if any) dedicated IT staff
- Cloud-everything
- Typically outsource large portion of IT function
- Managed Services Providers (MSPs) often provide most IT services
- MSPs complicate things (creating further dimensions of risk)

The Landscape

- This

- Not This

The Landscape



Systems Design

Technology Support

Technology Sourcing

SMB Tech Professional

“IT” Security

Attendee Poll

- SESSION: PDAC-T09

What Methods do you use for third-party assessments today?

Excel Spreadsheets!

Third-Party Ratings Firm

Internal Risk Team

Other

https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3875

The Landscape

Some of the obstacles with SMBs…

- Limited ability to validate responses
- Wildly inconsistent criteria in responses
- Little/no information on SMBs from rating's firms
- Lengthy process
- SMB contract value below 'critical' threshold

RSAConference2019

Looking from both sides

CASE STUDIES

Looking from both sides

CASE STUDIES: PREFACE

- All organizations profiled resolved deltas
- All materially impacted 3rd parties were informed and involved
- Engagement terms are in their own words
- The names of the guilty were (are) withheld….

RSAConference2019

Looking from both sides

Case Study #1 – Medical Payment Processor

Looking from both sides

CASE STUDY #1: Medical Payment Processor

- 35 person organization
- Payment processor for medical organizations
- Custom built web portal and payments app
- 2 dedicated IT staff
- 4 dedicated web developers

Looking from both sides

CASE STUDY #1: Medical Payment Processor

- “We have achieved high levels of compliance in the industry, including **HITECH Act, HIPAA, PCI** and **Red Flag**. This includes **PCI-DSS 3.1 SAQ-D** and **HI-TRUST level 5** compliant (Common Security Framework). In addition to an extensive internal auditing program, the company undergoes further audits by LexisNexis, American Express, MasterCard and Vantiv.“

Looking from both sides

CASE STUDY #1: Medical Payment Processor

QUALYS® SSL LABS

SSL Report: [redacted]

Assessed on: Fri, 28 Apr 2017 14:29:46 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

F

Visit our documentation page for mor

This server is vulnerable to th

This server is vulnerable to the Op

This server accepts RC

This server uses 64-bit block cipher (3DES / DES / RC2 / IDEA) with modern protocols. Grade capped to C. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

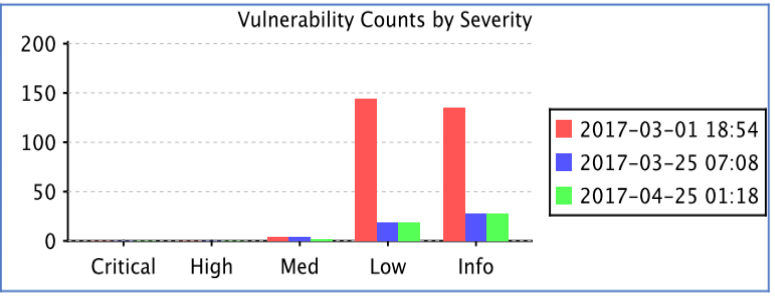
Trustwave®

Report Date: 2017-04-28

Vulnerability Scan Report: Executive Summary

Part 1. Scan Information

Scan Customer Company	[redacted]
ASV Company	Trustwave Holdings, Inc.
Scan Compliance Status	Fail
Date Scan Completed	2017-04-25
Scan Expiration Date	N/A



Looking from both sides

CASE STUDY #1: Medical Payment Processor

- **Findings:**
  - Compliance was a function of IT
  - High levels of turnover in IT
  - 16 month decline from ‘optimal’ compliance statements
  - Business was focused on improving website features
  - “DevOps can’t be slowed down with security”
  - Shoestring budget to fix issues

Looking from both sides

CASE STUDY #1: Medical Payment Processor

- **Findings:**
  - All statements were materially true, at one point…
  - Legitimate remediation efforts underway
  - Responding to 3rd party inquiries as if all certifications were “current”
  - Technical leadership ignorant of what risks were
  - Business leadership was insulated from declining assessment results

Looking from both sides

CASE STUDY #1: Medical Payment Processor

- **Changes Made:**
  - Created internal risk reporting matrix
  - Used material areas of PCI and HIPAA as evaluation points
  - Directly tied development roadmap to InfoSec posture
  - IT and DevOps budgets tied to security priorities
  - Forecasted two quarters forward

RSAConference2019

Looking from both sides

Case Study #2 – Defense Contractor

Looking from both sides

CASE STUDY #2: Defense Contractor

- 45 person organization
- Specialized manufacturing of defense-related items
- Subject to ITAR & SCI
- Extremely high value Information

Looking from both sides

CASE STUDY #2: Defense Contractor

- **Findings:**
  - Technology compliance was function of Operations
  - Extremely mature physical controls
  - Intense culture of security; focused on nation state (physical) threats
  - 2 person IT team; mostly focused on Industrial Controls
  - All tactical IT functions outsourced to MSP
  - “Zero failure” culture

Looking from both sides

CASE STUDY #2: Defense Contractor

- **Findings:**
  - Internal segregation of information met external requirements
  - MSP used 3rd party for all higher-level technical support
  - MSP had remote access to all non-air gapped systems
  - MSP used foreign nationals for 24x7 support
  - MSP was considered “trusted 3rd party” by subject firm

Looking from both sides

CASE STUDY #2: Defense Contractor

- **Findings:**
  - MSP introduced huge security risk
  - MSP introduced total of six previously unknown vendors
  - These vendors were operating / storing data in 5 countries outside the US
  - MSP made no differentiation between their clients' InfoSec requirements
  - No disclosure of outside parties by MSP to subject firm
    - The MSP referred to their "NOC Team" and "Monitoring Team"

Looking from both sides

CASE STUDY #2: Defense Contractor

- **Findings:**
  - MSP responded to all assessment questionnaires / 3rd party inquires
  - MSP had no consideration of their effect on the information risk equation
  - MSP conducted no internal ongoing training beyond end-user focused security awareness (“anti-phishing”)
  - “Zero failure” culture of security led to lack of transparency

Looking from both sides

CASE STUDY #2: Defense Contractor

- **Changes Made:**
  - Expanded scope of internal InfoSec program to include:
    - Clear understanding of End-to-End systems including all 3rd party vendors
    - “All parties” policy adherence & compliance
    - Two-party control and approval for firewall changes with external audit
  - Educated executive team to blind spots that led to the “situation”
  - Initiated cultural change from “Zero failure” to “perpetually improving”

RSAConference2019

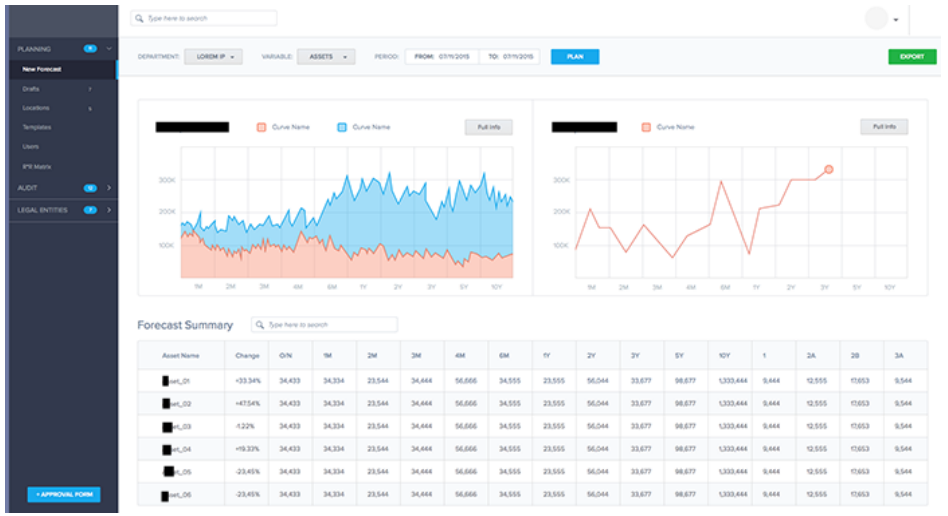
Looking from both sides

Case Study #3 – Financial Analysis Firm

Looking from both sides

CASE STUDY #3: Financial Analysis Firm

- 22 person organization
- Investor Relations portal for Alternative Investment industry
- Investor-specific Personally Identifiable Information (PII)
- Not subject to FINRA / SEC compliance



Looking from both sides

CASE STUDY #3: Financial Analysis Firm

- Findings:
  - Extremely high-value information under their management
  - Subject extremely aware of current InfoSec best-practices
  - Many prominent clients
  - Questionnaire response was “cut-and-paste perfect”

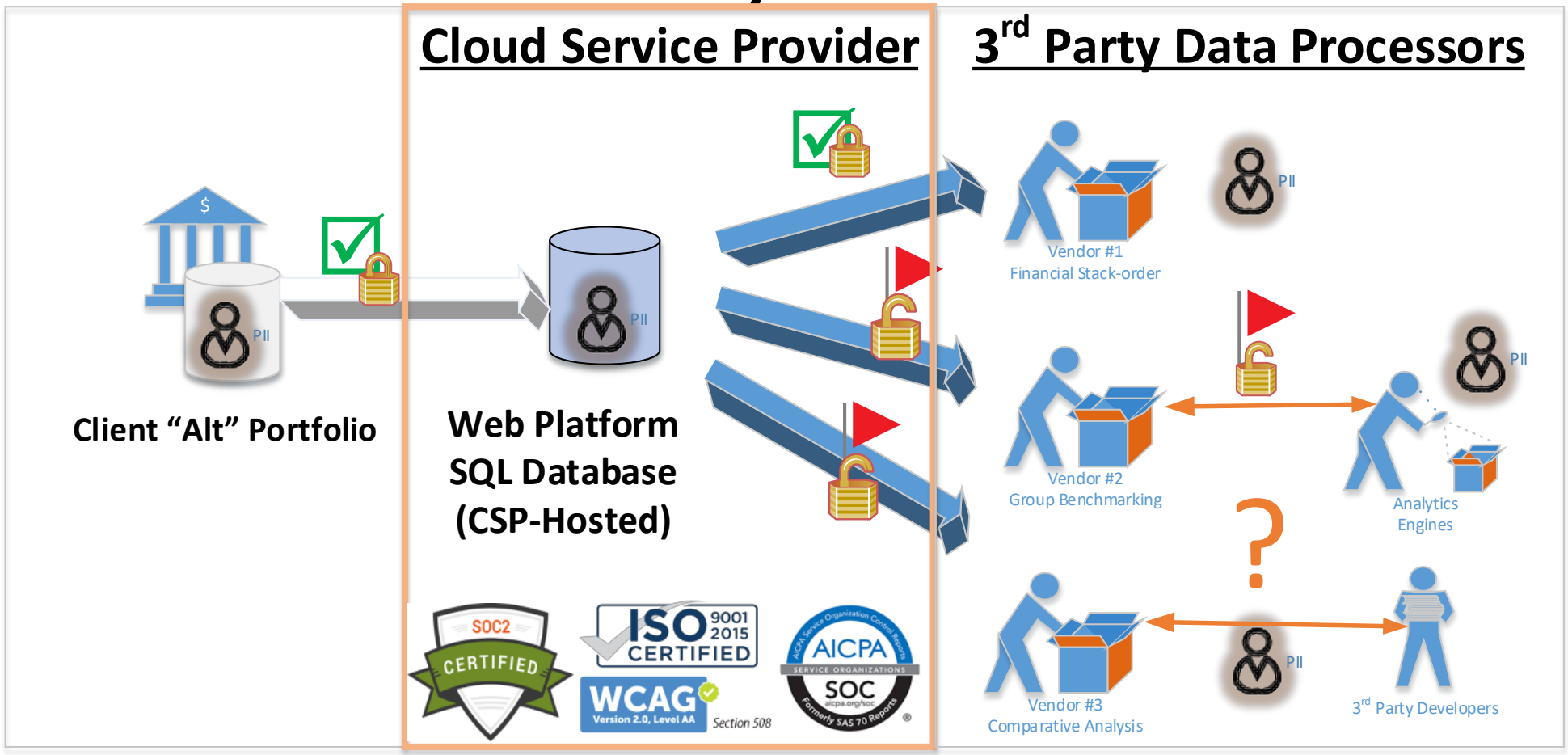
Looking from both sides

CASE STUDY #3: Financial Analysis Firm

- Findings:
  - Passed due-diligence of big names because of relatively low percentage of Assets Under Management (AUM) in ‘Alternative Investment’ portfolio
  - Mile-wide and inch-deep controls
  - Performing at minimum standards
  - “We’re a software company, not a data center”

Looking from both sides

CASE STUDY #3: Financial Analysis Firm



Looking from both sides

CASE STUDY #3: Financial Analysis Firm

- Changes Made:
  - Disclosure of specific Cloud Service Providers (CSP)
  - Disclose complete chain-of-custody of sensitive data
  - Proof of subscription services from their CSPs
  - Requirement of internal executive point of InfoSec accountability
  - Contractual requirement for all external (3rd party) compliance

RSAConference2019

Applying these lessons: Effective tools & techniques

Helping others while helping ourselves

Effective Tools & Techniques

COMMONALITIES IN THE SMB

- SMBs have **limited bandwidth** to think about security
- They are focused on only what is **required**
- Often ignorant of the **intention** of controls
- Overwhelming **culture of failure** for any “miss”

Effective Tools & Techniques

COMMONALITIES IN THE SMB

- The tools that key vendors (MSPs) use are **rarely considered**
- Risk stops within their organization
  - Universally no consideration for risk introduced by **their** vendors
- SMB Executives are willing to make changes

Effective Tools & Techniques

Tool #1: Change the conversation

- INTENTION
- MOTIVATION
- ACCOUNTABILITY
- EDUCATION

Effective Tools & Techniques

Tool #1: Change the conversation

- Convey both your **intention** and **motivation** for requiring specific controls
  - What are you specifically intending to secure, measure, mitigate
- **Educate:** Security is less an “IT” thing, more an executive thing
  - Require a named executive/owner sponsor to be **accountable** for the assessment
- Start from a position of cooperation & **mutual benefit**

Effective Tools & Techniques

Tool #2: Measure what Matters

- RELEVANT
- OBJECTIVE
- TRANSPARENT
- FEEDBACK

Effective Tools & Techniques

Tool #2: Measure what Matters

- Is every SMB vendor subject to the same requirements?
- Focus inquiry to the most **relevant** areas of risk
- Start with broad frameworks
- Iterative **objective** measurement cycles

Effective Tools & Techniques

Tool #2: Measure what Matters

- Risk measurement is likely new to most SMBs
- Provide **transparency** in your assessment & results
- Communicate in **business terms** on shortcomings

Effective Tools & Techniques

Tool #3: Excellence Awarded

- BENCHMARK
- RECOGNIZE
- REPORT
- REPEAT

Effective Tools & Techniques

Tool #3: Excellence Awarded

- SMBs are highly competitive
- Tie security performance with contract terms (their profit)
- Peer competition influences change
- Many enterprises recognize vendors in their supply chain today

Effective Tools & Techniques

Tool #3: Excellence Awarded

- **Recognize** objective improvements
- Create a **tiered** cybersecurity recognition program
- Very time-limited recognition
  - E.g. “1H 2018 Small Business Cyber-Security Excellence Award”
- A SMB will likely not perform equal to larger businesses

Effective Tools & Techniques

Tool #3: Excellence Awarded

- **Communicate** your changing landscape & requirements
- Help them help themselves
- Answer their questions
  - They likely could never afford access to your cyber/risk resources

Attendee Poll

- SESSION: PDAC-T09

Do you have a cybersecurity vendor recognition program today?

Yes

Not Yet!

No

I Don't know

https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3850

RSAConference2019

Applying these tools
(Operationalizing your SMB cybersecurity initiatives)

APPLYING THESE LESSONS

- When you return:
  - Identify if you have demographics information of your vendors
  - What percentage are SMBs?
  - Start the internal conversation of recognition / contract terms for SMBs
- Over the next month:
  - Review assessment responses from your SMB vendors
  - Any commonalities? Anything stand out?
  - Identify the core risk areas that your SMB vendors increase exposure
- In the next quarter:
  - Create one or more SMB-sized risk assessments
  - Iterative in nature; 10-20 questions max.; Focus on core risk areas.

APPLYING THESE LESSONS

- Over the next year
  - Establish a cybersecurity recognition program for vendors
  - Educate and equip SMB executives on the use of tool(s) most appropriate to their business & your need
  - Educate them on their need to assess their MSPs / CSPs
  - Re-assess your SMB vendors using your new iterative assessment methodology
  - Provide feedback on their assessment scores
    - Share how they compare with other similarly sized vendors

“Understanding is a two-way street….”

-Eleanor Roosevelt

RSAConference2019

Interested in learning more?

Small-Group Session

March 7th

7:00am – 7:50am

Moscone West 3009 Table C

Improving outcomes of due-diligence with small businesses

RSAConference2019

Questions? Feedback?

Lawrence Cruciana **@lcruciana**

Corporate Information Technologies

lcruciana@corp-infotech.com

RSAConference2019

Thank You!

RSAConference2019

Tools & References

Effective Tools & Techniques

- References & Tools for later use
  - CIS 20 Controls

    https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf

  - Vendor Security Alliance (VSA)

    https://www.vendorsecurityalliance.org/questionnaire2018.html

  - NIST CSF

    https://www.nist.gov/cyberframework/small-and-medium-business-resources