RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-M01**

Supplier Risk: Throw Out the Old playbook!

Heidi Pili

Security Director, CDW
@HeidiPili

Tim Wainwright

CEO, Security Risk Advisors
@TimWainwright

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

These are the views of the presenters and are not the opinion or position of their respective organizations.

Today

Current state of industry practices

Changing our Mindset

A New Approach

Gameshow!

Takeaways

Supplier Risk Hype

REUTERS®

Microsoft says new breach discovered in probe of suspected SolarWinds hackers

SINCLAIR BROADCAST GROUP

AP Sinclair hit by ransomware attack, TV stations disrupted

Ransomware attack disrupts Toronto's public transportation system

CBS NEWS

solarwinds

SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments

REUTERS®

T-Mobile litigation over major data breach to proceed in Missouri

Marriott INTERNATIONAL

Marriott Fined $23M for Data Breach That Hit Millions

200 million Facebook, Instagram, and Linkedin users' scraped data exposed

COLONIAL PIPELINE CO.

AP Major US pipeline halts operations after ransomware attack

Current State

1000’s of suppliers

Several 100’s of questions in SIG, SIGlite and commercial “Exchanges”

Scorecard services

Compliance frameworks reinforce the questions

Supplier Risk team resources

Parts of the risk assessment process performed in isolation

Warnings about change

Password Policy was WRONG for a very long time

- 8 characters
- Special, upper/lower, numbers
- Lockout after 3 attempts
- **Change every 60 days**
- Etc

Controls deployed because of compliance frameworks

- What control worked its way into PCI-DSS in 20xx and still lives as a result?
- Point solutions: Database Access Monitoring, Web App Firewalls

Warnings about change

Let’s not make
the same mistakes

Change our mindset

What do we really want from our suppliers?

Change our mindset

How can we
get out of our own way
to do this better?

Change our Mindset: What do we really want from our Suppliers?

1. **Sustain their services to our organization!**
2. **Don’t let our data get breached!**

And what this really means is we don’t want them to get **ransomed and extorted**.

If we can focus on this central idea, we can free ourselves from many, many weak habits.

Evolve our Mindset: Compliance → Threat

"Compliance-driven"

- ✓ ITGC's & Audit playbook
- ✓ Assets, Identity, Business Continuity
- ✓ *Identify, Prevent, Restore mindset*

ISO 27001

"Threat-driven"

- ✓ Blue & Red playbook
- ✓ Ransomware resilience
- ✓ *Detect & Respond* mindset

MITRE | ATT&CK®

Thirty Questions

The principles of our 30 Questions activity are to:

1. **Increase speed and focus.** Security cannot be a bottleneck. We want to respond with a fast but thoughtful recommendation to our business partners when they are looking at a new supplier. We also want to be able to go back and effectively assess a larger number of our existing suppliers.

Thirty Questions

The principles of our 30 Questions activity are to:

2. **Only ask meaningful questions.** We will only ask consequential questions where a negative outcome substantially increases our risk. We are focused on the ability to detect and respond to intrusions, prevent and restore from ransomware attacks, and sustain production services.

Through this approach, we hope to…

Thirty Questions

The principles of our 30 Questions activity are to:

3. **…Help these partners.** Many of them are less sophisticated in cybersecurity, and we want to help them avoid being breached or ransomed for their sake and ours

Thirty Questions

Throwing out the old playbook meant starting from scratch

We thought about what mattered most to thwart adversaries

We added the right level of detail to the questions

We considered what can be evidenced vs. just stated

We went back to NIST and ISO to make sure nothing essential was missing

The CISO can modify and approves these questions

Thirty Questions

Examples

Do privileged users have separate administrator and user accounts?

Yes, your supplier is more likely to get infected by malware and ransomed if they don’t do this.

Examples

Do you terminate access for employees and contractors within 24 hours of their departure?

Your supplier won’t get ransomed because of this.

Examples

Do you use multi-factor authentication on all Internet-facing services?

Better:

Do you use multi-factor authentication on all Internet-facing services including:

- ❑ Email
- ❑ VPN/VDI
- ❑ Cloud Environments
- ❑ SaaS Applications
- ❑ Remote support tools
- ❑ File transfer
- ❑ Websites
- ❑ None of the above


30
Worthy

Thirty Worthy Themes

Question Hints

- If the answer is No, the supplier would already be out of business
- The question doesn't translate to enough ransomware or data breach risk
- We know they will answer Yes but we don't believe them
- We care a lot about how they harden and test network and endpoint visibility
- We care a lot about how they practice incident readiness

Do you perform 24x7x365 continuous security monitoring and response:

- ❑ In-house
- ❑ Outsourced
- ❑ Co-Managed
- ❑ None of the Above

If 2 or 3, who is the provider?

WORTHY

Do you use industry standard data center physical access controls?

NOT WORTHY

Do you use a CMDB to maintain asset information including criticality levels?

NOT WORTHY

Do you test a documented Incident Response Plan in a tabletop exercise at least annually?

Do you use firewalls to filter inbound traffic to your network?

NOT WORTHY

Do you regularly audit your firewalls configurations and rules?

NOT WORTHY

What is the patching goal for your emergency vulnerability process?

- ❑ < 48 Hours
- ❑ < 7 Days
- ❑ < 14 Days
- ❑ < 30 Days
- ❑ None of the above

WORTHY

Do you have cloud security configuration monitoring enabled (GuardDuty, Azure Security Center, or third-party tool)?

WORTHY

Does your password policy require the following (Select all that apply)

- ❑ 8-12 characters
- ❑ Complexity and numbers
- ❑ Changes per NIST guidance
- ❑ 3-5 attempt lockout
- ❑ 5 password history

NOT WORTHY

Do you require all users to have unique user accounts with complex passwords which must be changed on first use?

WORTHY

Do all employees and contractors receive annual security awareness training?

WORTHY

Do you use Data Loss Prevention (DLP) to monitor storage and transfer of our data?

NOT WORTHY

Which of your backup solution's recommended hardening capabilities do you use to protect your backups?

- ❑ Snapshots
- ❑ Immutable Snap Locks
- ❑ Air Gap
- ❑ Use of Local Accounts
- ❑ MFA for admin access to the console
- ❑ Other
- ❑ None of the above

Do you conduct annual tests of restoration from backup capabilities for systems supporting services to our organization?

WORTHY

Please attach your independent SOC2 report, not older than 12 months.

NOT WORTHY

Have you documented the authorized locations and users and flows of our data in your network in a data flow map?

Will you notify us within 24 hours of a breach or compromise involving our data?

NOT WORTHY

Intermission & Case of Study: Simplifying TPRA

- Using Standard Information Gathering (SIG) Lite. ~330 questions
- Average time to execute each assessment was 113 days!
- Security breaches continue to happen out there
- A new, more practical approach was required to effectively assess our vendors
- We re-defined our approach to TPRA, including related questionnaires
- We also asked for help
- Our current TPRA questionnaire includes less than 40 questions
- Average time to execute each assessment is now 18 days
- Our TPRA process will be working as a ‘system’ where the questionnaire is connected to other elements of the process
- Our Legal department and key stakeholders welcomed and support this approach

Do you have a “report phishing” button that any employee can use to trigger investigation by your 24x7 CyberSOC?

WORTHY

Do you have a documented Secure Systems Development Lifecycle Policy (SSDLC) that governs how security is built into your application(s)?

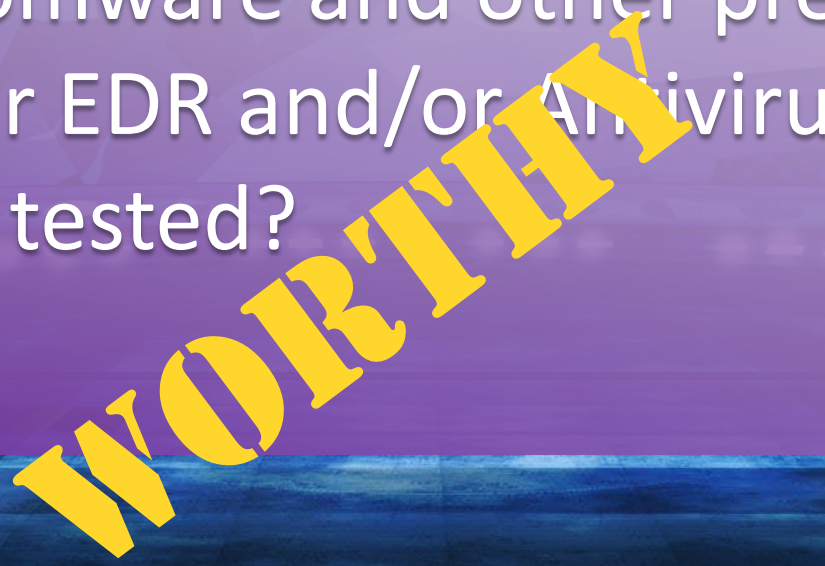
NOT WORTHY


Do you use a service to alert you to leaked credentials, encryption keys, session tokens and sensitive data?
WORTHY

Does your 24x7x365 CyberSOC use one of the following Endpoint Detection & Response platforms on your servers and workstations?

- ❑ Microsoft Defender ATP
- ❑ Crowdstrike
- ❑ Elastic
- ❑ SentinelOne
- ❑ Other
- ❑ BlackBerry Cylance
- ❑ Carbon Black
- ❑ FireEye
- ❑ None of the Above

Have the ransomware and other prevention settings of your EDR and/or Antivirus been turned on and tested?



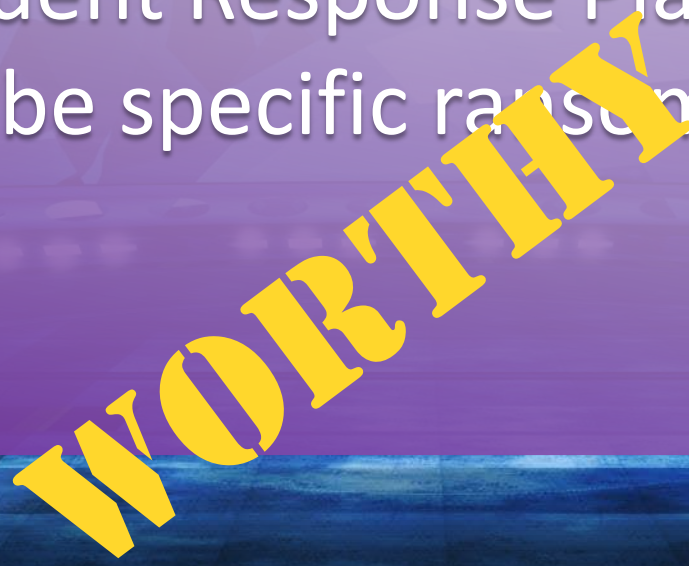
Do you have a privacy policy and are you compliant with CCPA?

NOT WORTHY

Do you use industry standard data center environmental controls?

NOT WORTHY

Does your Incident Response Plan and tabletop exercise describe specific ransomware response procedures?



Do you use secure file transfer methods to share our data with authorized third parties?

Challenges

Your team members will resist this approach

We need to increase the skill of our team members who assess suppliers.

Some suppliers may resist our approach because they have already completed the 400+ questionnaire for their other customers and our questions yield real gaps.

Bring your supplier risk management stakeholders and process together.
Contracts, Privacy, any score/ratings services or third-party attestations you decide you need.

Thinking Ahead

GRC as a Threat-Driven Function – what will it take?

- Technical upskilling: Cloud, MITRE, more
- GRC = a robust Blue Team
- Extend Supplier Risk to “Ecosystem Security” and use this approach for due diligence on M&A’s
- Leaders: take a rotation in SecOps and Cloud

Takeaways

- Information overload is not good risk management
- GRC and Supplier Risk teams need to:
  1. Not expect a different risk outcome if you don't change what you're doing
  2. Evolve their mindset to be more threat-driven
  3. Let go of those old chestnuts
  4. Change their approach to be consultative not "auditative"
  5. Upskill their team

Application & To-Dos

- Create business case for changing supplier risk program *(improved risk management, increased speed and coverage of suppliers)*
- Obtain feedback and buy-in from Legal, Compliance, other stakeholders
- Review 30 questions, make them your own, and create your tools for the process *(workbook, supplier communications, workflow)*
- Create skills inventory and development plan for supplier risk team
- Develop supplier risk calendar with prioritized “friendly” *(early-adopter)* suppliers