G2M
RESEARCH

How to Take a 360 Degree View of Cybersecurity

A G2M Security Webinar

Tuesday May 25, 2021

SecurityScorecard

Crowe

Webinar Agenda

9:00-9:05	Ground Rules and Webinar Topic Introduction (G2M Research)
9:06-9:35	Sponsoring Vendor presentations on topic
9:36-9:41	Panel Discussion Question #1
9:42-9:42	Audience Survey #1
9:43-9:48	Panel Discussion Question #2
9:49-9:49	Audience Survey #2
9:50-9:55	Panel Discussion Question #3
9:56-10:03	Audience Q&A (8 minutes)
10:04-10:05	Wrap-Up

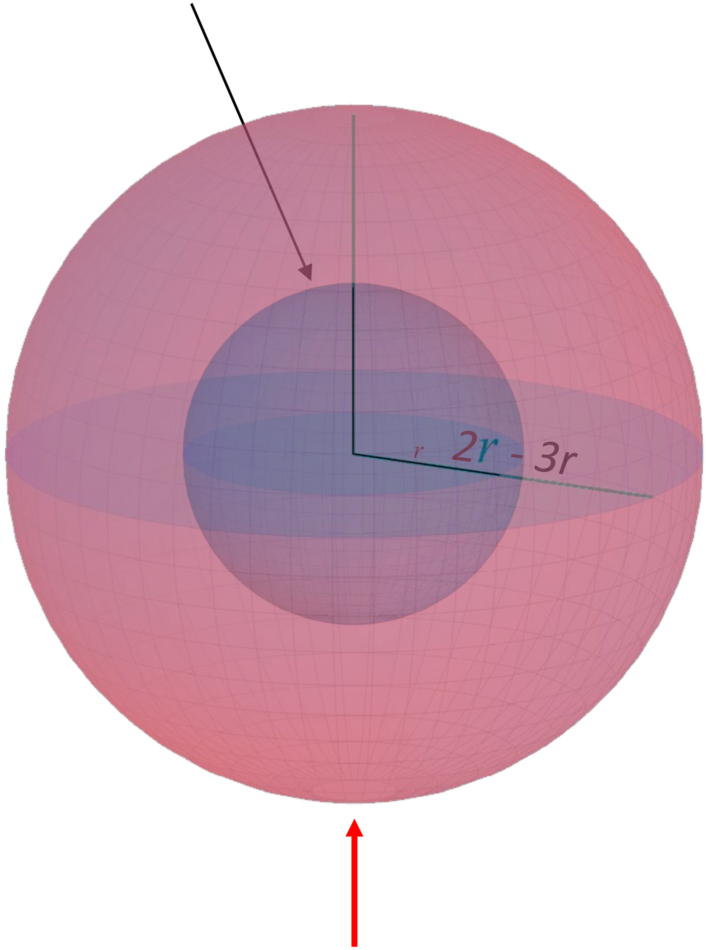
G2M Research Introduction and Ground Rules

Mike Heumann
(Managing Partner, G2M Research)

Your Risks Are Not Just Hackers and Ransomware…

- Cybersecurity risks are usually opaque
- Cybersecurity risks are often beyond arms reach
- Think about the SolarWinds Hack
  - Malware authored/inserted by 2nd level subcontractor
  - Affected companies were buying software from a mature, trusted vendor
  - Bad security practices contributed to the exploit
  - Affected a large number of companies, gov’t agencies
- While 3rd party risk management is (somewhat) new, it is a vast attack surface

Traditional IT Attack Surface



The New Enterprise Attack Surface

Top Challenges to IT Implementing Effective 3rd Party Risk Management*

G2M RESEARCH

1. Getting an accurate picture of the security landscape
2. Meeting demands for reporting and compliance
3. Automation/integration of 3rd party risk into security stack
4. Budget constraints for new areas like 3rd party risk
5. Scaling limited SecOps budget to cover 3rd party risk
6. Expansion of # of critical vendors in risk mgmt portfolio
7. The growing sophistication and volume of cyberattacks
8. Rapidly expanding compliance and regulatory reqm'ts

** G2M Research Public Survey October 2020*

Panelists

G2M RESEARCH

SecurityScorecard

Shaun Walsh
Vice President,
Product Marketing
www.securityscorecard.com

Crowe

Jill Czerwinski
Partner – 3rd Party Risk Team
www.crowe.com

Crowe

Morgan Strobel
Sr. Manager, 3rd Party Risk Team
www.crowe.com

G2M RESEARCH

Mike Heumann
Principal Analyst
www.g2minc.com

Audience Survey Question #1

What is your role in third party/vendor risk management (check all that apply; answers are anonymous):

• I am responsible for assessing and/or managing third party risk:	33%
• I support the third party risk program but I am not responsible for it:	11%
• I manage vendor relationships and vendor communications:	0%
• No direct responsibility, just interested in the topic:	56%

SecurityScorecard

Shaun Walsh

Vice President

Product Marketing

www.securityscorecard.com

What are the odds of…

Being Eaten
by a Shark

1 in 3,748,067

Getting Struck
by Lightning

1 in 960,000

Experiencing a
Data Breach

1 in 4

Why 1 in 4 Experience a Security Breach?

People Peep Clicking

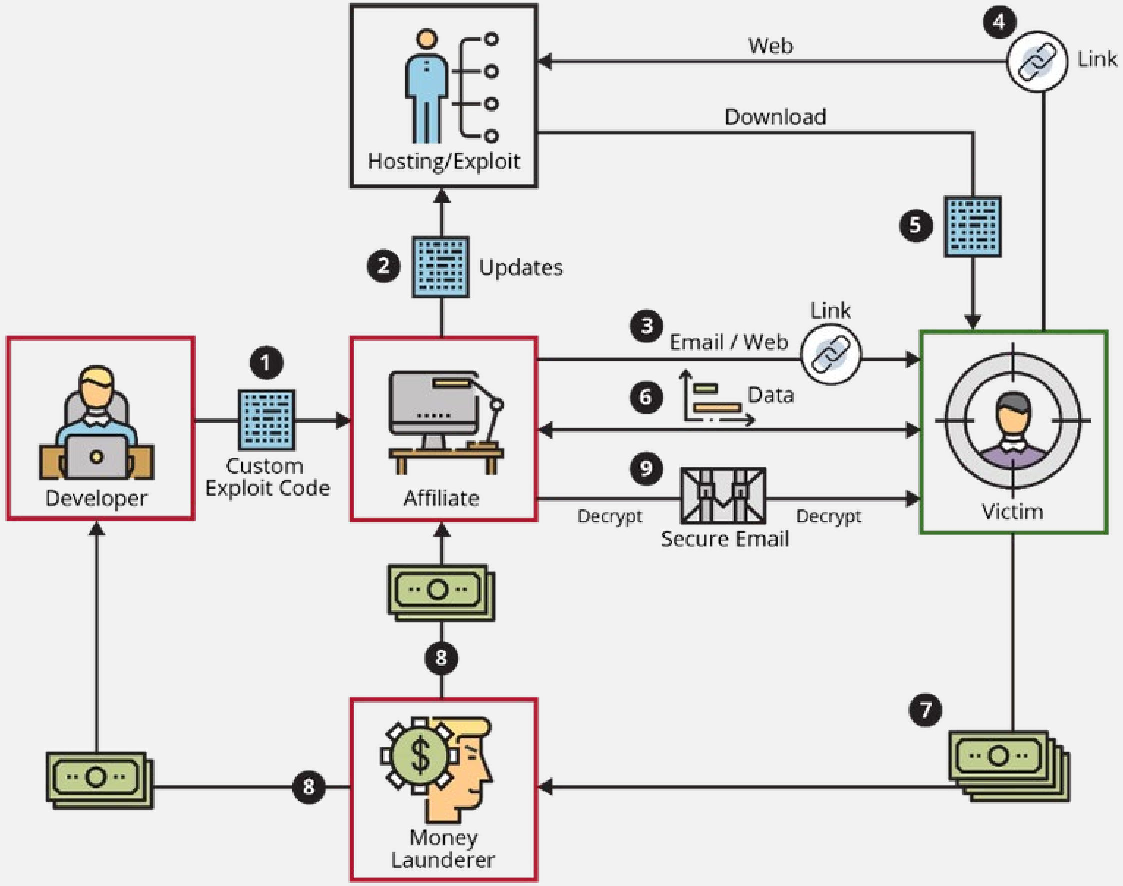
Patches and Upgrades

It's a Business Model

Expanding Threat Landscape

It is a Business Model…Not a Hack

- Nation states
- Criminal organizations
- Ransomware-as-a-Service
- Motives not technology drive threats



5 Challenges for Modern VRM

1 Digital Transformation & remote work are expanding threat land scape

2 Continuous monitoring of internal, 3rd and 4th party ecosystem risk

3 Global expansion of regulatory, compliance and reporting demands

4 Scaling staff, patching/revision management and budgets

5 Aggressive nation state and criminal organizations

Crowe

Jill Czerwinski,
Morgan Strobel
3rd Party Risk Team
www.crowe.com

Tackling the Third-Party Cyber Risk Problem:

Practical options to manage risk.

G2M Presentation

May 21, 2021

Crowe

Now that we’ve confirmed the risk… Lets discuss our options.

Negotiate a favorable contract.

Leverage cyber ratings data.

Perform a traditional assessment.

Monitor issues & risks.

Negotiate a favorable contract.

Minimum Standards for Cybersecurity

- Key expected controls defined, usually in an appendix
- Redlines inform deviations from expected controls.

Requirement for Independent Testing

- They must have a thorough evaluation each year and provide the report.
- SOC, PCI, ISO, HITRUST, FedRAMP etc.

Right to Audit and Investigate

- Right to audit at least annually, with a third party if desired
- Right to follow up with prompt response to a vulnerability or alert.

Leverage cyber ratings.

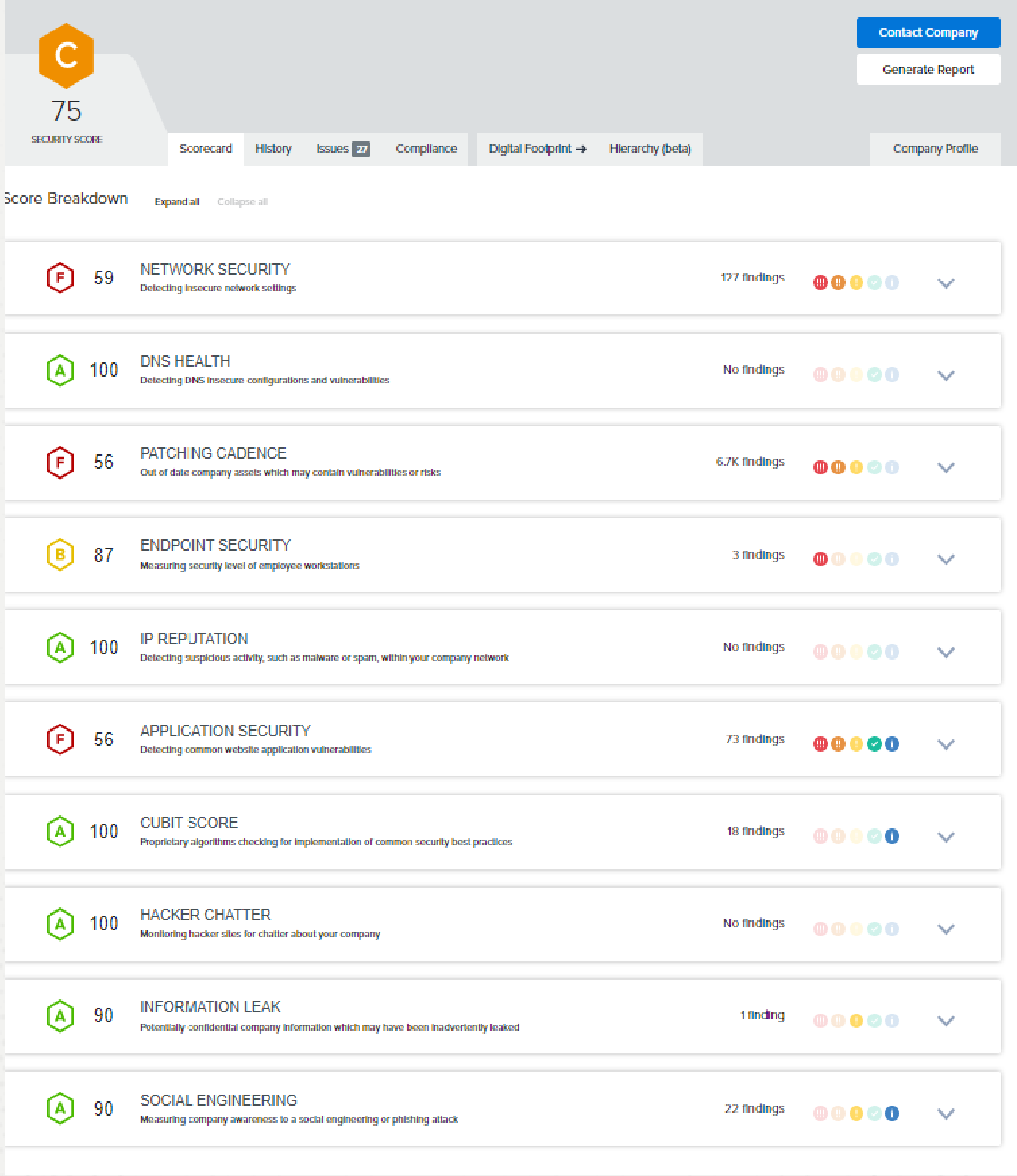
Provides an outside-in view.

Empirical data not subject to manipulation or bias.

Should be considered an overall indicator of posture.

Can be used to start a dialogue.

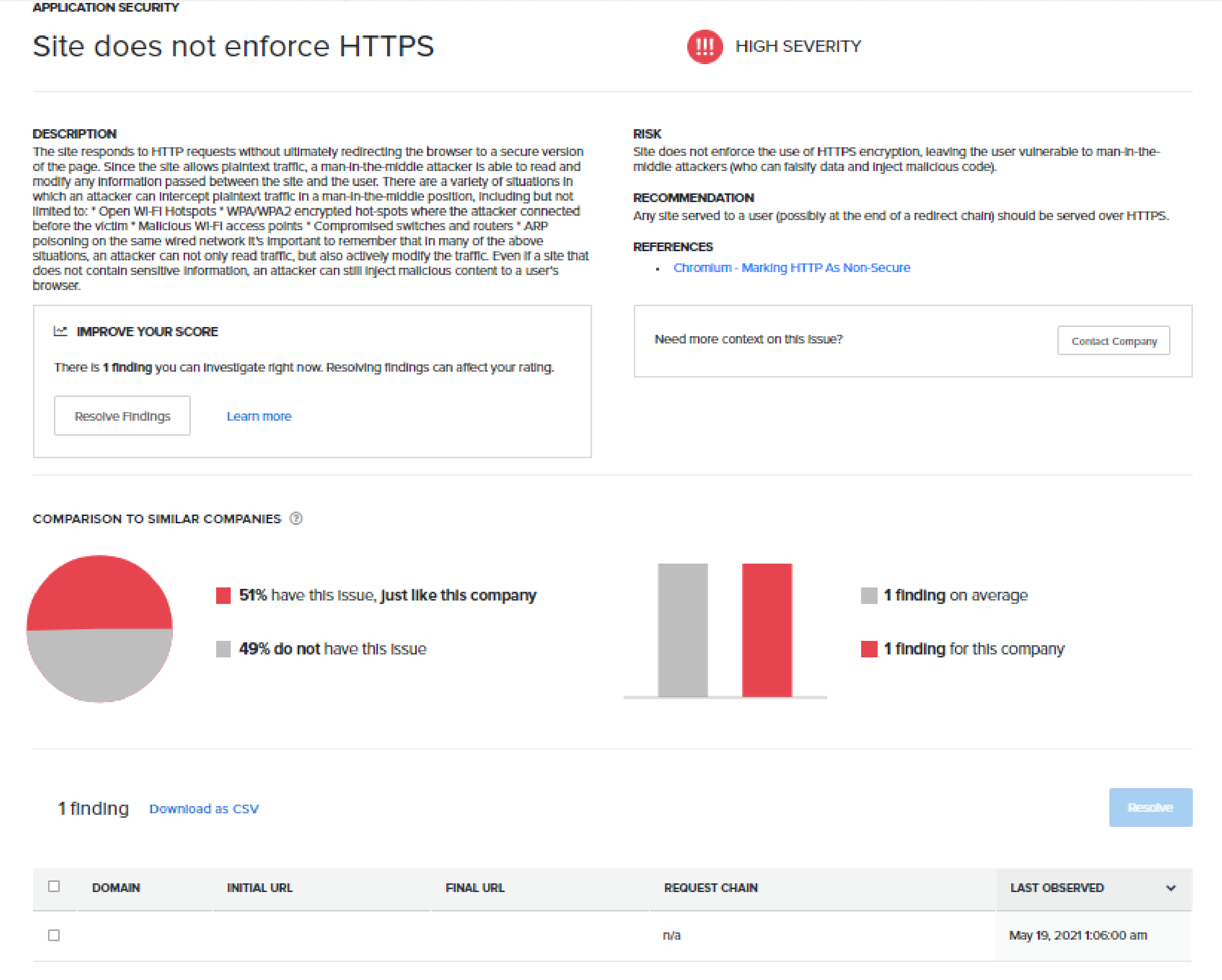
Leverage cyber ratings.



75
SECURITY SCORE

Score Breakdown Expand all Collapse all

F	59	NETWORK SECURITY Detecting insecure network settings	127 findings
A	100	DNS HEALTH Detecting DNS insecure configurations and vulnerabilities	No findings
F	56	PATCHING CADENCE Out of date company assets which may contain vulnerabilities or risks	6.7K findings
B	87	ENDPOINT SECURITY Measuring security level of employee workstations	3 findings
A	100	IP REPUTATION Detecting suspicious activity, such as malware or spam, within your company network	No findings
F	56	APPLICATION SECURITY Detecting common website application vulnerabilities	73 findings
A	100	CUBIT SCORE Proprietary algorithms checking for implementation of common security best practices	18 findings
A	100	HACKER CHATTER Monitoring hacker sites for chatter about your company	No findings
A	90	INFORMATION LEAK Potentially confidential company information which may have been inadvertently leaked	1 finding
A	90	SOCIAL ENGINEERING Measuring company awareness to a social engineering or phishing attack	22 findings



APPLICATION SECURITY

Site does not enforce HTTPS

!!! HIGH SEVERITY

DESCRIPTION

The site responds to HTTP requests without ultimately redirecting the browser to a secure version of the page. Since the site allows plaintext traffic, a man-in-the-middle attacker is able to read and modify any information passed between the site and the user. There are a variety of situations in which an attacker can intercept plaintext traffic in a man-in-the-middle position, including but not limited to: * Open Wi-Fi Hotspots * WPA/WPA2 encrypted hot-spots where the attacker connected before the victim * Malicious Wi-Fi access points * Compromised switches and routers * ARP poisoning on the same wired network It's important to remember that in many of the above situations, an attacker can not only read traffic, but also actively modify the traffic. Even if a site that does not contain sensitive information, an attacker can still inject malicious content to a user's browser.

RISK

Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).

RECOMMENDATION

Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.

REFERENCES

- Chromium - Marking HTTP As Non-Secure

IMPROVE YOUR SCORE

There is **1 finding** you can investigate right now. Resolving findings can affect your rating.

Need more context on this issue?

COMPARISON TO SIMILAR COMPANIES

🟥 **51%** have this issue, **just like this company**

⬜ **49% do not** have this issue

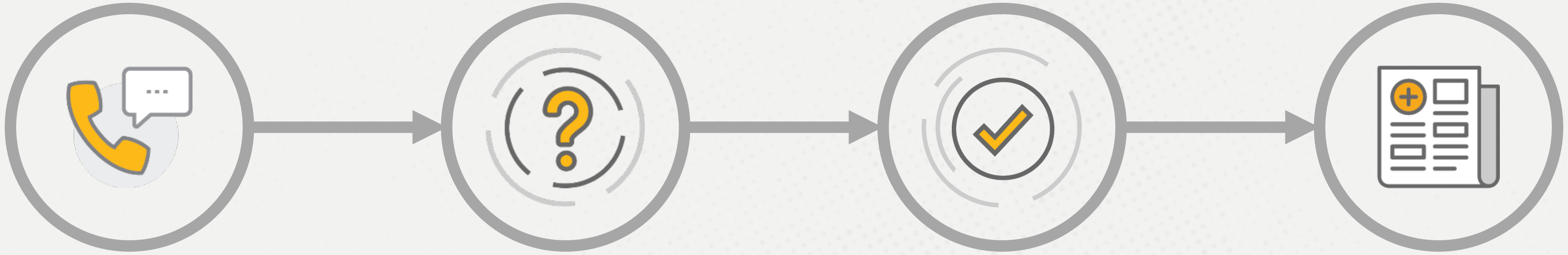
⬜ **1 finding** on average

🟥 **1 finding** for this company

1 finding Download as CSV

□	DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
□				n/a	May 19, 2021 1:06:00 am

Perform a traditional assessment.



1. Plan
2. Inquire
3. Check
4. Report

Perform a traditional assessment.

Pro tips:

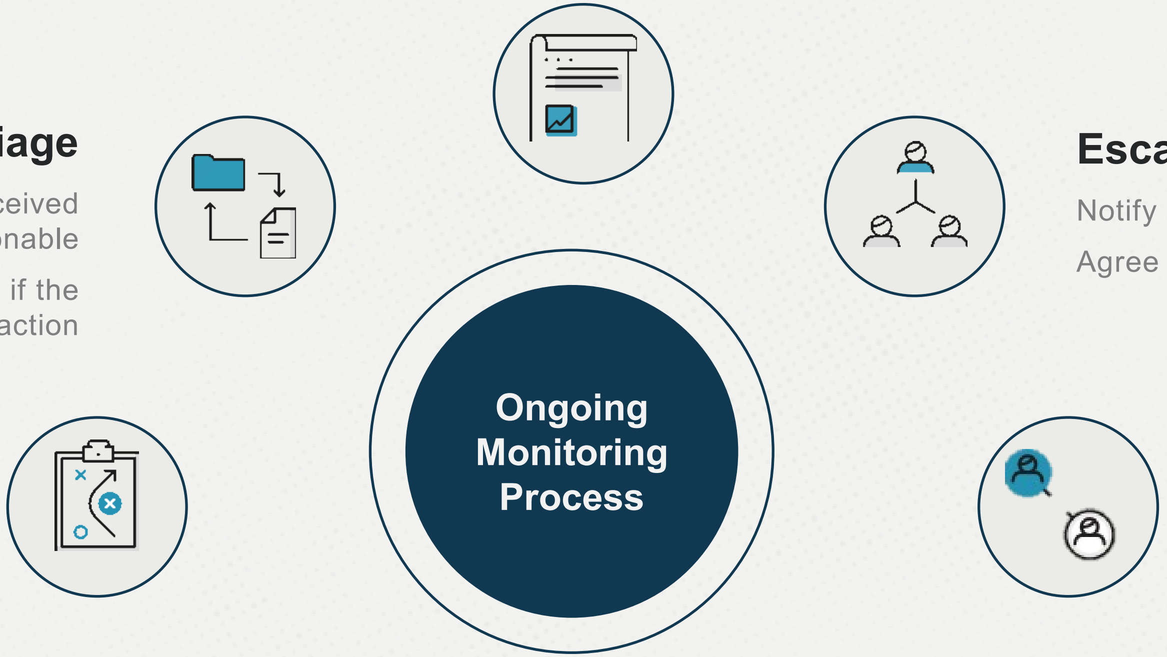
Less is more:
Only ask if you care about the answers.

Engage:
Don’t underestimate the power of a call with the vendor.

Validate:
Without proof the assessment is flimsy.

Nobody’s perfect:
No issues? you may be missing the mark.

Monitor issues and risks.



Review

Gather more information about the context and risks

Engage with SMEs and the third party

Triage

Define how you will record that you received an alert and whether the alert was actionable

Based on defined criteria, determine if the alert requires action

Escalate

Notify affected parties of the risk

Agree upon action plans to correct

Plan

Who will you monitor, for what risks, and with what feeds?

Define when and how you will receive notification and who will act

Track

Monitor the closure of the risk

Leverage issue management systems where appropriate

Panel Questions and Audience Surveys

Panel Question #1

Clearly 3rd party-based attacks are prevalent and increasing. If I am in a small organization, am I still at risk?

- Shaun Walsh (SecurityScorecard)
- Jill Czerwinski (Crowe)
- Morgan Strobel (Crowe)

Audience Survey Question #2

G2M RESEARCH

To what extent does your organization have a 3rd party risk assessment plan/practice (check one; answers anonymous):

• We continuously assess 3rd party risk:	20%
• We assess 3rd party risk on a periodic (annual or better) basis:	20%
• We assess 3rd party risk when bringing on all new vendors:	0%
• We have assessed 3rd party risks after security incidents:	0%
• We are exploring implementing a 3rd party risk program:	20%
• We are too small to consider 3rd party risk:	0%
• Don’t know:	40%

Panel Question #2

How do you intelligently decide which 3rd party vendors to look at when assessing risks?

- Jill Czerwinski (Crowe)
- Morgan Strobel (Crowe)
- Shaun Walsh (SecurityScorecard)

Audience Survey Question #3

How “close” have you been to a 3rd party-based breach (check one; answers are anonymous):

• Our company has had a confirmed 3rd party-based breach:	66%
• We have had a 3rd party vendor that suffered a breach:	0%
• We have used products that were breached:	0%
• We don’t know whether we have had a 3rd party breach:	0%
• We can confidently say we have not had a 3rd party breach:	33%

Panel Question #3

What factors should enterprises look at when choosing a 3rd party risk assessment partner?

- Morgan Strobel (Crowe)
- Shaun Walsh (SecurityScorecard)
- Jill Czerwinski (Crowe)

Audience Q&A

Thank You For Attending!