Current State

1.) How do cybersecurity professionals think about “risk” in relation to their environment?

2.) How do they understand/learn about risk? (tools or processes for example)

- What do you do with information about risk?

Future State

- How, if in any way, do they anticipate their view of risk evolving in the next 2-3 years?
- How, if in any way, do they anticipate using risk measures differently in the next 2-3 years?

Goals of Research

Short term

To learn more about how cybersecurity professionals think about risk and the problems they face when trying to understand and take action related to risk.

Long term

To determine which use cases for Full Stack Risk should be prioritized including integrations between Rapid7 products, application risk score, and more.

Participant Screening Questions

1. What is your role/title?
2. Which of the following technologies do you or your team work to secure? [participants must have 4 from this list]
    1. Traditional data center infrastructure
    2. Cloud infrastructure (IaaS or PaaS)
    3. Containers
    4. Operational Technology infrastructure (OT)
    5. Endpoints (ie: desktops, laptops, smartphones)
    6. Applications
    7. Microservices and APIs
    8. I’m not sure
3. Does your company develop its own applications and software? [~half should develop their own applications]
    1. Yes
    2. No
4. [if yes] What percentage of your applications are internally developed?
    1. ~10

    2. ~25
    3. ~50
    4. 75 or more
5. [If yes] Which of the following reflects the types of applications your company builds? [select all that apply]
    1. My company builds public facing applications used by clients and customers.
    2. My company builds applications for internal use only.

Interview Script

Thank you for participating in our research session today! My name is Adrienne, I'm a User Experience Researcher here at Rapid7. Right now, I'm working with our product team to better understand the experience of cybersecurity professionals and how they measure, report and most importantly communicate about cyber risk across the organization's attack surface.

During this call, I will be asking you a series of open ended questions related to risk. There are no right or wrong answers to any of the questions I'm going to ask; we are looking to understand your perspective and gain some insights into how practitioners are managing cyber risk. I may ask you to clarify concepts or terminology because my background is in research vs. deep cyber security expertise just to make sure we have a full understanding of the topics we'll cover.

I have a few colleagues on the phone who will be taking notes for this session, and may help me provide context as necessary or have questions they want to ask as well as we're talking. And lastly, I always like to record if possible so that I don't miss anything. Is it OK if I record our session for internal use?

Begin Recording

I'd like to start with a few background questions to get some context about your role.

Background

1. I saw from the sign up form that your title is [x] is that right?
2. How long have you been in your current role?
3. What is the name of the team that you're on?
4. How many people are on your team?
5. In terms of your day to day work, what are your formal responsibilities as [role]?

Security Team Structure

1. **We have a few questions about your security team specifically.**
    1. Can you describe the structure or organization of the security team?
2. **How many people are on the team/sub-teams?**

1. [If not mentioned]: Do you have a person/team dedicated specifically to Cloud Security?
2. Do they report directly into the information security team or are they organizationally a separate team/individual? What are their responsibilities?
3. [if not mentioned]: Do you have a person/team dedicated specifically to application security?
4. Same question we covered with cloud, are they part of the information security team and what are their responsibilities?
5. Is there anything that you would change about the structure of your security team, if you could?

3. **Can you tell me more about that?**
    1. [optional probe]: Is this structure effective given current conditions - pandemic, remote workforce, cloud and digital transformation programs, etc?
    2. Do you work with any managed service providers?
        1. [if yes]: Can you tell me more about that?
        2. What is the MSSP contracted to deliver?

Risk Management & Reporting

1. Now I'd like to ask you a few perceptual questions about "risk" within the context of a cyber security program. Does your organization have a formal or consistent definition of cyber risk? Soc, identity, architecture.
    1. [If yes]: What is it?
    2. [If not] How would you personally define "cyber risk"?
    3. Do other teams or functions outside of your immediate team define or measure cyber risk differently?
2. Does your cyber program use a security framework like NIST, ISO, MITRE for example?
3. Does your organization have an Enterprise Risk Management program, where business risk of all categories is inventoried and treated by an executive team?
4. [If so]: Is cyber risk its own component or category within that program?
    1. [if not] Is there anything in particular that you think works well about cyber risk being excluded from the ERM program, or on the contrary, any challenges that it presents?
    2. Are the people who make up the ERM board/program also tasked with making cyber security related decisions? [ie: budget, resource allocation, prioritization and security initiatives]
    3. Can you share an example or two of some of the topics that have recently been posed to the group/team to decide?
    4. How was it determined that those topics should be brought to the ERM board? (What are the criteria? Is it based on a dollar threshold or other criteria?)
5. Now I have a few questions about the definition of "attack surface" and how you think about attack surface management. Over the past year or two, you've probably noticed that the cyber security vendor market and analysts started to distinguish the "external attack surface" and define "attack surface management" to only include hosts and

applications outside an organization's perimeter. Could you tell me how you define "attack surface", and whether those definitions/references align with your perspective?

6. Does the larger security team align itself and its day to day responsibilities the same way (external vs. internal)?
7. Can you help me understand the functions or capabilities within your cyber program and how risk is tracked and reported across those functions? (for example, SOC, VM, Application Security, etc)
8. Are there specific categories or ways that you organize risk reporting? - dont report on doing well. Top 10 things to worry about
    1. Why do you organize risk reporting in that way?/Can you tell me more about that?
9. I'd like to ask you a few questions about the measurement of risk. Can you give me a sense of the metrics that you use to measure cyber risk?
    1. When it comes to reporting or measurement of cyber risk, what do you share with executives and your board?
       Would you be willing to show me a sanitized version of your reports or dashboards for context?
    2. What metrics do you use to measure the security team's performance
        1. Are there different measures for different security functions (ex. SOC, VM, Application Security, etc)?
10. How much of a priority is it for your organization to improve communication and measurement of cyber risk across the enterprise to executives or the board? You can give this to me on a scale of 1-5 where 1, if it hasn't been prioritized vs. other needs and 5 is its top priority.
    1. Can you tell me why you gave that rating? With this question we are trying to understand how consistent the demand across industries and verticals is, along with an understanding if organizations believe cyber risk management is too subjective and squishy to solve.
    2. Can you share the organization's security projects or initiatives in the near-term to improve the organization's ability to measure, manage and report on cyber risk? Do any of these initiatives include something specific to improve cyber risk communication?
        1. Note taker: What are the subjective or qualitative goal(s) of their security program? What are the quantitative goals?
    3. Has the priority changed at all over the past 6 months?
        1. Can you tell me more about why?
        2. Are there any specific initiatives in place to help the organization communicate a consolidated measure of cyber risk that you're able to discuss?

Risk Comparison/Prioritization

15. Now I'd like to give you a scenario. You have limited time and money, and you have a few areas of your security program that you'd like to invest in, and leadership is asking

you for justification. How would you determine where you should focus and how would you justify that to leadership?

    1. What factors do you consider in order to prioritize your investment? - direct business impact-- prove to our customers that they can trust us, help us with rfp. Peers are doing this. Million dollar investment 50 million investment
    2. [probe] What specific information or criteria do you use to decide what risk to address or prioritize?
    3. Why is that information important to your ability to prioritize investments in your security program?
    4. How do you go about getting that information?
    5. What works well about that [process]?
    6. What challenges do you face with that [process]?
    7. [probe] Earlier we also talked about security frameworks. Does the security framework you use play a role in how you weigh different types of investments in your security program?

16. Do you have a way of quantifying or understanding the *overall risk* across your entire attack surface?
    1. [if yes] What formula(s), tools or processes do you use to achieve overall risk? [if so] Is that process manual or automated?
    2. [if yes] How does the organization use the overall assessment of cyber risk?
    3. [if yes] What works well about your current overall risk assessment?
    4. [if yes] What challenges do you have with your current overall risk assessment?

Communicating Risk

17. Once you understand overall risk and it's prioritized, what do you do with that information?
    1. Who do you have to communicate with or report to about cyber risk? board - impacted clients, strategy to change the culture, macro level nist csf. Weekly - leadership, informal - anything worthy of noting. Bitsight score. Compliance. Onboarding and off-boarding. Monthly - graphical top 10 risks.
        1. [For note taker]: Note Senior management, Middle management, individual contributors
        2. How do you go about describing risk to those people?
        3. What works well about this process of communicating and reporting about cyber risk?
        4. What challenges do you face when communicating and reporting about cyber risk?
18. What decisions are made (or actions are taken) as a result of the communications?
19. Is there specific data or data type(s) that would aid you in closing those challenges in communicating and managing cyber risk?

Evolving View of Risk

20. For you, what would the ideal capability be for measuring, reporting and managing cyber security risk? This assumes you have unlimited budget and time to operationalize this capability.
21. Who else do you know who would be a good candidate for this research.