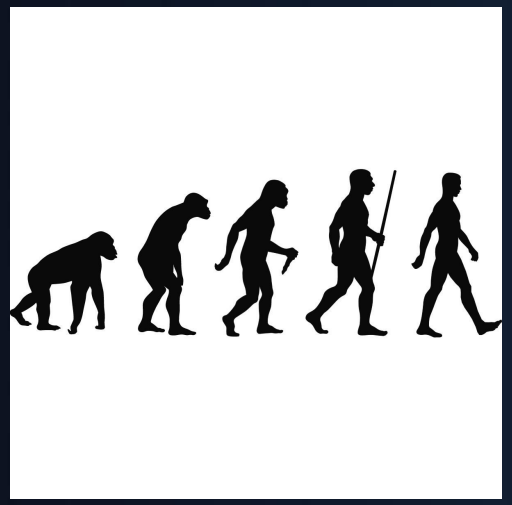


The evolution of our profession

Jack Freund
FAIR Institute

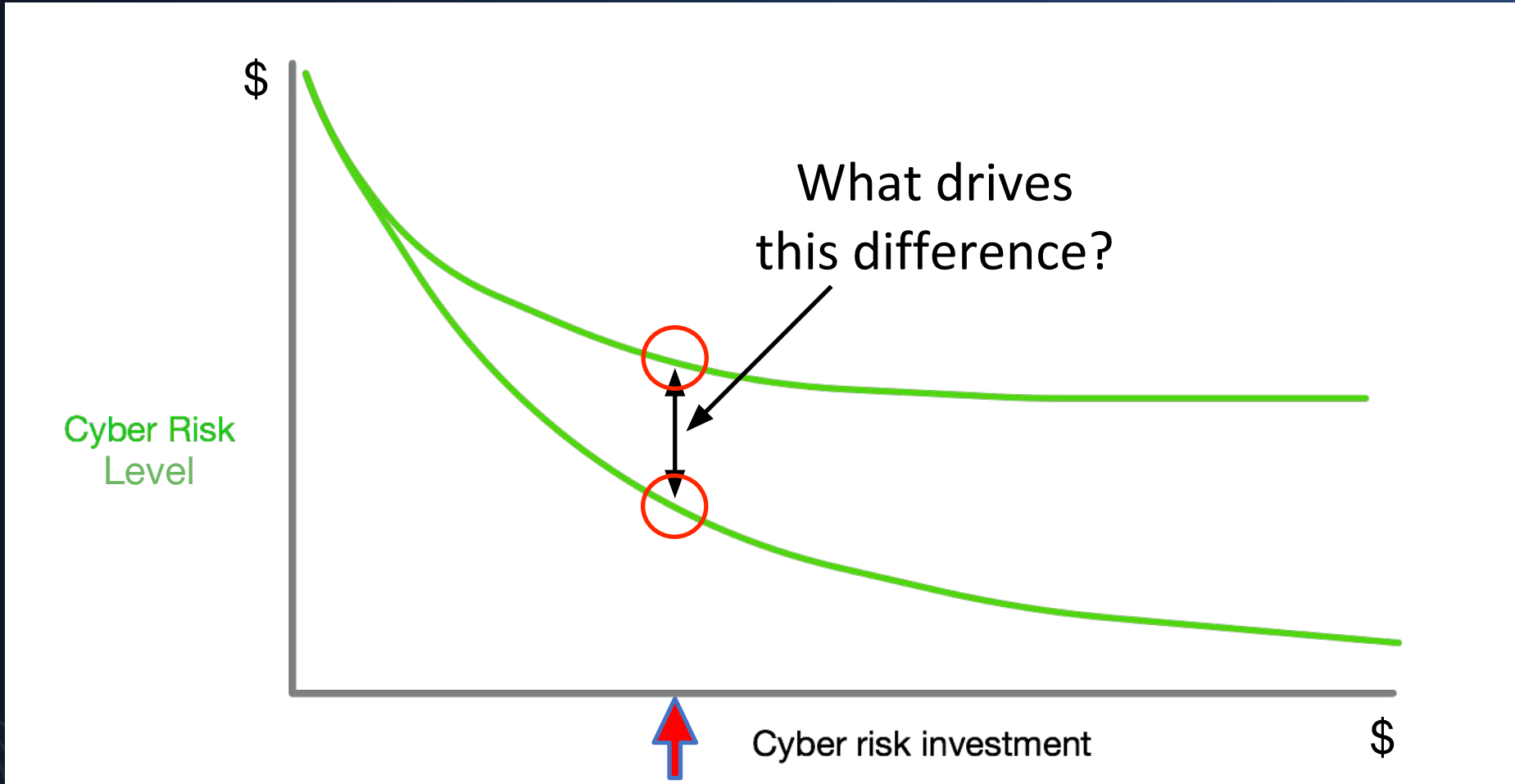
The Epochs of Information Security

	Mainframe 1960's - 1980's	PC 1980's - 1990's	Internet 1990's - 2000's	Cybersecurity 2000's - 2010's	Cyber Risk 2010's —>
Threat Landscape	• Employees (error & maliciousness)	• PC Viruses	• Network-enabled attacks • Online vandalism	• Cyber criminals • Hactivists	• Nation-state actors • Artificial intelligence
Tools	• CA Top Secret • RACF	• Policies • Antivirus	• Firewalls • Vuln scanners • Pen-testing • Awareness trng.	• MSSPs & SIEMs • Forensics • Industry regulations	• Red/Blue teams • Global regulations • ML & Artificial intelligence
Role / Perception	• IT worker bee	• Distinct job in IT	• Distinct infosec department in IT • Birth of the CISO • Office of "NO"	• Enterprise programs • Separate budgets • Board reporting	• Board priority • Risk manager • Business enabler • ERM function
Measurement & Decision Support	• SLA's	• Mental models • Ordinal scales	• Mental models • Ordinal scales • FUD	• Mental models • Ordinal scales • Maturity models • FUD	• Economic analysis • Data science

What is the cost of a $5,000,000 cybersecurity program*?

*Salaries, benefits, services, technologies, etc.

Why it matters…



Decisions

How cost-effectively we apply our risk management resources.

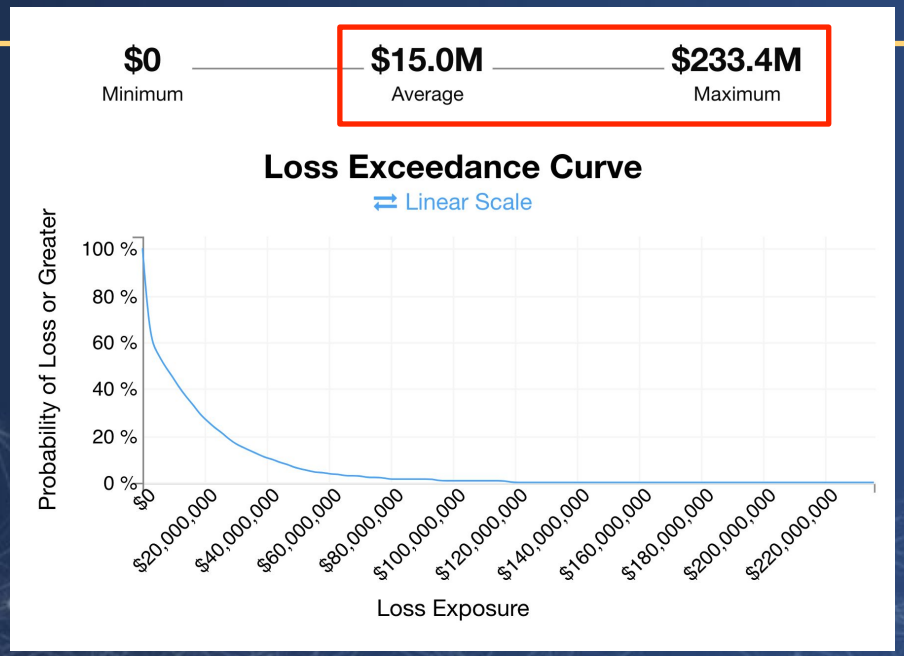
Prioritization example

- A vulnerability scanner identifies a web application with a SQL injection weakness. The scanner's scoring model (CVSS) labels the weakness as "critical".
- Software development resources are redirected from other work to correct this weakness.
- However, this application is: a) not Internet-facing, b) requires authentication in order to find and exploit the SQL injection flaw, and c) doesn't have access to sensitive information.
- If the organization had postponed remediation, it is extremely unlikely to experience a significant loss event. Therefore, resources could have been better applied to other, higher-risk concerns.

Prioritization example

An audit discovered that privileges are not consistently being updated for user accounts with access to a customer service application containing credit card numbers.

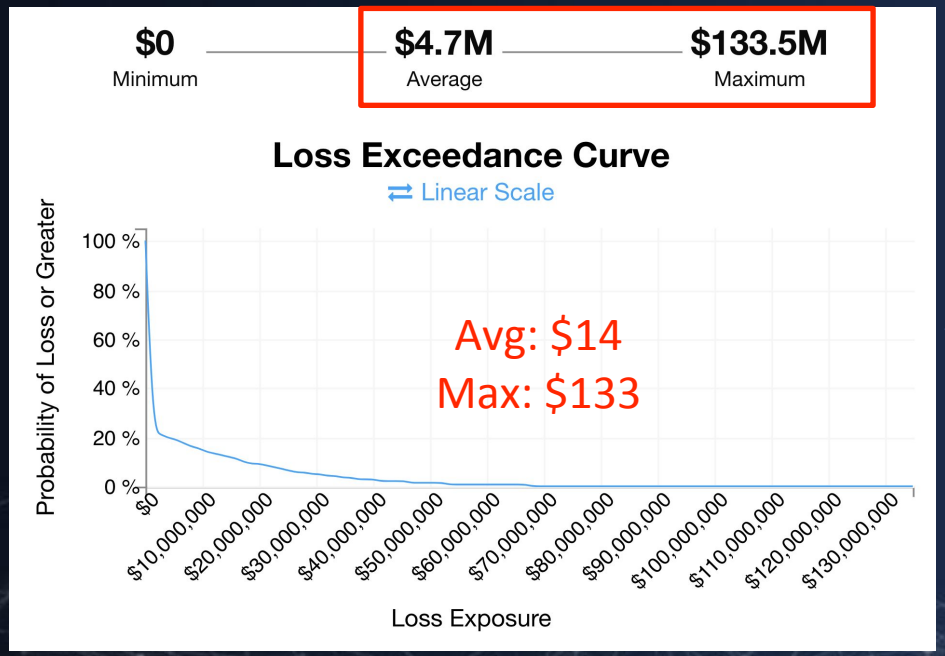
A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.

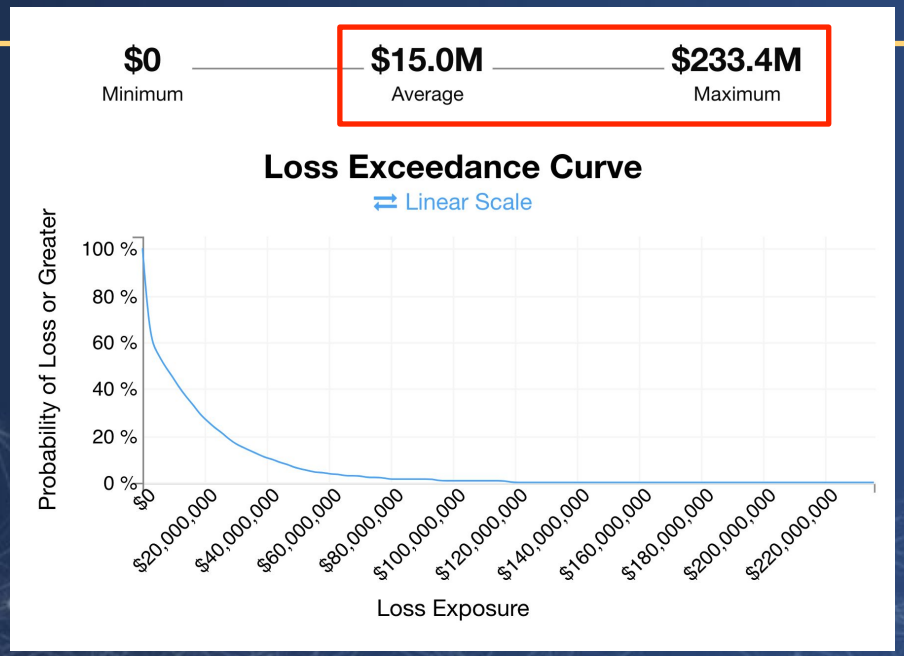


Cost-benefit example

A risk reduction solution was identified that was going to cost $750k in year 1, and approx. $300k yearly thereafter.

A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.





Focus example

- The “cloud”
- E-mail
- Reputation
- Phishing
- Ransomware
- Internet of things (IoT)
- Insiders
- Patching
- Shadow IT
- Technology debt

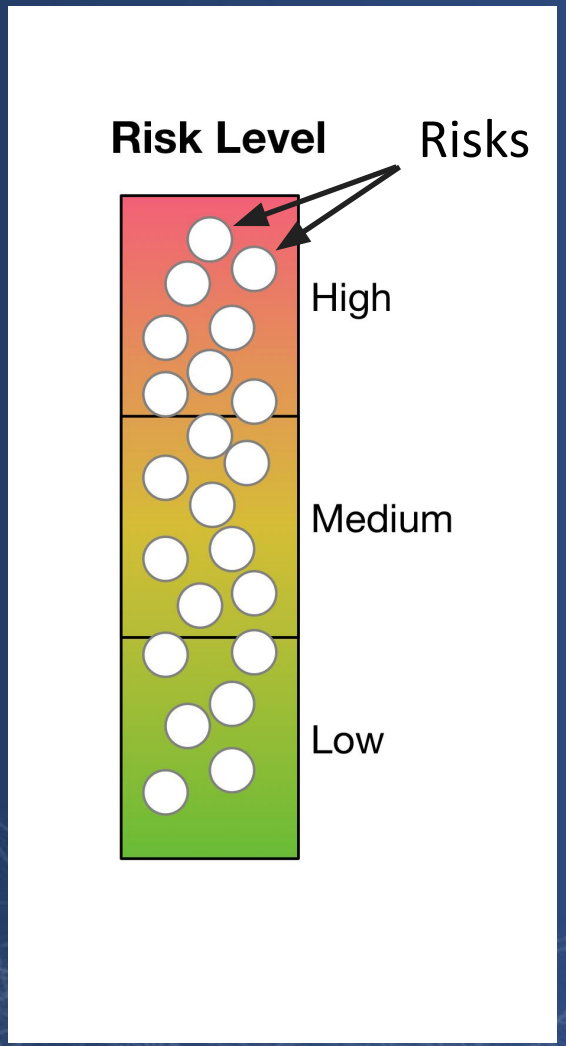
What is expected to happen when top risks have been identified?

Some “simple” questions…

- How much more risk does the highest “high” represent than the lowest “high”? (And do we even agree on which one is highest?)
- How much more risk does the lowest “high” represent than the highest “medium”?
- How much risk is there in aggregate?
- Why are the lines drawn where they are?

Are these reasonable questions?

How would you defend your responses?



The risk landscape in a nutshell…

Complex

Dynamic

Limited Resources

Which means…

Organizations must be very good at prioritizing their cyber risk problems and solutions.

- The future of cybersecurity is cyber risk management
- Cyber risk management is inherently quantitative, requiring economically-based prioritization and cost-benefit analyses

Your bottom line…

Questions?