Harvard Business Review

WEBINAR SUMMARY

Why Executives Underinvest in Cybersecurity

Featuring Alex Blau

DECEMBER 13, 2017

SPONSORED BY VARONIS

WEBINAR SUMMARY

Why Executives Underinvest in Cybersecurity

PRESENTER:

Alex Blau, Vice President, ideas42

MODERATOR:

Angelia Herrin, Editor, Special Projects and Research, *Harvard Business Review*

Overview

Despite the growing threat of potentially costly cyberattacks, companies are still underinvesting in proper security. Often C-suite executives outside of the technology teams see cybersecurity as a limited problem that requires risk mitigation and specific solutions, and not a continual process that needs ongoing risk management.

Behavioral science can help technologists, like the chief information security officer (CISO), understand why many senior executives don't view security threats the same way they do. They can also use this knowledge to persuade the CEO and other executives to rethink and perhaps invest more in cybersecurity.

Context

Alex Blau discussed the behavioral science behind why people make decisions. He shared ways issues can be reframed so that executives may be more likely to manage cybersecurity risks.

Key Takeaways

Behavioral economics offers insight into why people make decisions.

Behavioral economics blends behavioral science with economics to provide a framework for how and why people act and make decisions. This approach offers a more emotional, human side to decision making than the traditional economics rational actor model, where a person is expected to unemotionally, logically, and rationally weigh costs and benefits to make an optimal decision.

Using behavioral economics, ideas42 identified four reasons executives underinvest in cybersecurity:

- Different ways of describing and thinking about risks.
- Opposing mental models.
- Overconfidence in investments.
- Attention on the wrong things.

Reframe risks in vivid terms to give executives a better understanding of the problem.

The first behavioral reason for underinvestment in cybersecurity is that a CEO may have a very different understanding of the problem and risk than a more technical person, like the CISO. Reframing risks in vivid organizational and business terms—especially in ways that show how the company is at risk—creates a better understanding of problems.

Example: Reframing risk as an organizational problem

CYBERSECURITY PROBLEM	ORGANIZATIONAL PROBLEM
Legacy servers are unpatched—and cannot be patched—so they need to be replaced or else risk an attack.	Legacy servers are where the accounting system lives, and if that system goes down we'll lose all of our critical financial data.

Formation of risk committees is an important step to articulate organization risks for senior executives. A risk committee is a team of executives or direct reports from multiple departments who can provide information on how the risk impacts the organization as a whole, and not just the IT team.

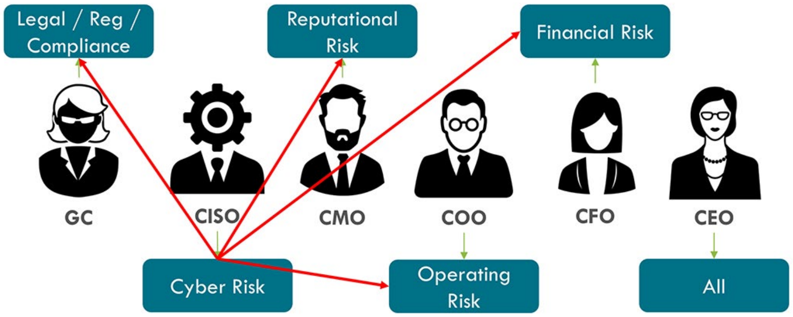

FIGURE 1: BUILDING RISK COMMITTEES TO SHARE CONCERNS AND PRIORITIES

> "Cyber risk is not something that's isolated to a specific quadrant of the business. We use technology throughout our operations . . . therefore cyber risk creeps into all of these other areas."
>
> —Alex Blau

Use metrics to refocus the discussion on what cybersecurity looks like.

Mental models help people quickly synthesize chaos and complexity to make predictions about the future. Because people bring their past experiences and knowledge to the model, it can result in oppositional mental models, which can lead to disagreement in how to move forward. Discussions can be refocused by using metrics to show what is happening in the real world.

When a CISO thinks about cybersecurity, they are often envisioning a complex solution that needs to be managed, where success is finding and fixing vulnerabilities, not just stopping breaches. The CEO, thinking about the same topic, may be thinking in terms of mitigation, where success is complying with industry and government regulations and not having any security breaches.

Metrics provide real-world feedback into the mental model, sharing information about bugs and vulnerabilities found and fixed, intrusion detection statistics, and other aspects of the cybersecurity process. Using this data, the CISO can show the CEO how successful cybersecurity is and how it relates to the complete management process.

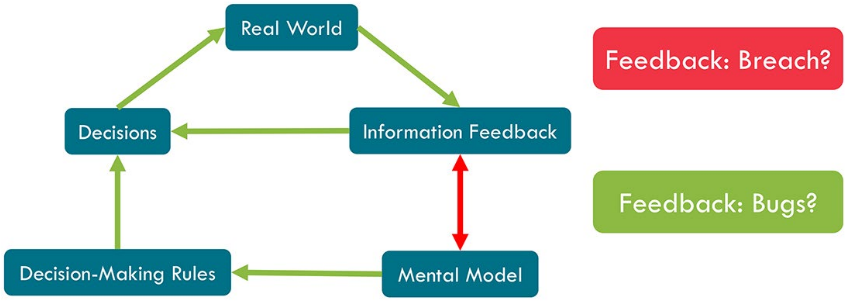

FIGURE 2: USING FEEDBACK TO REFRAME METRICS FOR SUCCESS

Clear security benchmarking against similar firms can combat overconfidence.

With more than half of companies saying their cybersecurity programs are better than average—while obviously only 50% can be above average—Blau believes there is overconfidence in cybersecurity investments. This overconfidence can be challenged with benchmarking against similar firms to see how the company is really performing.

Showing the business how it is performing in relation to its peers gives a realistic view of how its security investment fares. It also allows firms to share best practices, as well as current risks, which can lead to an improvement of security among all of the companies participating in benchmarking.

> "Being able to see what other people are doing—especially your direct peers—and the decisions and actions they're making can directly influence the decisions and actions that you take."
>
> —Alex Blau

Benchmarking can include infrastructure decisions, as well as the operations decisions being made and some of the key performance indicators (KPIs) of interest.

Break the system to expose vulnerabilities.

Actively attempting to break the system to expose vulnerabilities can help refocus attention from the wrong things to those that could play a role in the success of the security system.

Alongside unhelpful mental models, availability bias plays a role in centering attention on the wrong things. For example, news stories on viruses and security breaches focuses the CEO's attention on these external threats when, in reality, most successful attacks are coming from internal security problems, such as weak passwords, phishing attacks, system bugs, and poor development of security operations implementations.

Breaking the system refocuses attention on the actual problem areas by showing what vulnerabilities actually exist, and allowing the organization to identify and prioritize resolutions.

- **Penetration testing and bug bounty programs find vulnerabilities and bugs.** Once found, these flaws need to be fixed to close holes.
- **Attack key decision makers using internally initiated, safe attacks.** When executives fall for attacks, such as a phishing scam, it shows that anyone in the organization is vulnerable and encourages them to invest in solutions that prevent these attacks.
- **Test employees and behaviors and develop metrics showing how they respond to phishing scams and other security threats.** Results could lead to improved security processes and identify focal points outside of annual awareness training events.

Additional Information

- Deep Thought: A Cybersecurity Story tells a fictional—but true-to-life—cyber crime story that uses behavioral insights to show how a breach happened. The story is based on ideas42 research, using more than 60 expert interviews and over 120 research articles, funded by a grant by the William and Flora Hewlett Foundation.

Alex Blau is a Vice President at ideas42 currently focusing on challenges in consumer finance, design and decision making, and international development. Prior to joining ideas42, Alex worked as a research analyst at Tufts University's Friedman School of Nutrition Science and Policy, examining the exit strategies of a number of large, Title-II funded integrated nutrition interventions in Kenya. In addition, Alex has extensive experience developing agricultural supply chains for small-scale organic farmers in the Caribbean. Alex holds an MSc in food policy and applied nutrition science from Tufts University, and a BA in political science with a focus in international relations from Brown University.

Angelia Herrin is the editor for special projects and research at *Harvard Business Review*. Her journalism experience spans 25 years, primarily with Knight-Ridder newspapers and *USA TODAY*, where she was the Washington editor. She won the Knight Fellowship in Professional Journalism at Stanford University in 1990. She has taught journalism at the University of Maryland and Harvard University. Prior to coming to HBR, Angelia was the vice president for content at womenConnect.com, a website focused on women business owners and executives.