THE SILEO GROUP

CYBERSTAKES STORYBOARD™

Fixing cyber risk isn't just a technology game, it is a social game. It depends on more than firewalls, end-point protection and the IT Department. It depends on the human beings that wield the technology. Organizations continue to increase their security budgets at breakneck pace, and yet, cybercrime and breach continue to grow. Why? Because most have fallen into an unhealthy pattern of focusing on the technology at the expense of what's really at stake: the critical business activities that the technology supports. Technology is just one piece of a much larger story.

The Cyberstakes Storyboard™ is an organization, prioritization and communication tool that provides a narrative framework to connect your most valuable activities as a business to the data, systems, threats, adversaries, solutions and human beings that will help you avoid or minimize the most costly attacks. The Storyboard breaks the cyber risk plot into nine elements.

The key is to build one plotline at a time; to focus on one business activity, one adversary, one method of attack, one action plan at a time. By isolating each threat plotline to its own Storyboard, you will be forced to prioritize your highest-stakes activities and threats first. When complete, you'll have a simple narrative that can be communicated among your people, no matter their technical aptitude or position within the organization. In short, you will have a story that weaves initiatives, budgets, departments and technologies into an effective culture of security. Start by answering the following questions to isolate the critical areas you should focus on first.

DEFEAT

1. ANTICIPATE YOUR HIGHEST-STAKES DEFEAT FIRST

DEFEAT

Unlike how most stories are told, the Storyboard starts with the end in mind. Not coincidentally, this is how many movies are constructed, starting with the initial Defeat or conflict and progressing backwards to the beginning and onwards toward the end. Shift your focus from the technology and pay attention to what's actually at Stake. A series of "What if" questions of key stakeholders (e.g., What if we lost access to these systems for a month?) can help flesh out worst-case scenarios.

DEFEAT

What's the worst defeat you can imagine from a cyber attack? What is the most likely defeat you can imagine? What if it were successful?

GUIDE

2. CHOOSE A MORE QUALIFIED GUIDE THAN THE MEDIA OR YOUR GUT

The most secure organizations bring together a cross-functional team to Guide the Storyboard process. From inside of the organization this probably includes functional or operational leaders, the IT department, Human Resources, subject experts and specialists, and possibly Risk, Compliance and Legal. Often, the Board of Directors will provide oversight, and 3rd-Party vendors will add external expertise and support.

GUIDE

Who has the clearest view of the critical business activity (Stakes) that you seek to protect? What stakeholders should be involved on the Storyboard team to make sure that the greatest vulnerabilities are addressed?

ACTION PLAN

3. BUILD A STRATEGIC ACTION PLAN. NOT AN I.T. "ATTACK/ RESPONSE" LOOP

ACTION PLAN

To build an effective strategic Action Plan, you need to look beyond existing technology, previous attacks and resulting countermeasures. You need to be honest about how you currently approach the threats you face. It is important to determine whether or not you have been caught in the "Attack/Response" Loop. And then you need to consider, in advance, Steps 4-9, and outline an Action Plan.

ACTION PLAN

How many of your current cyberdefenses were implemented with specific, prioritized business activities in mind? Do you currently approach your defensive measures from a business perspective as well as a technical perspective? Where are you applying bandaids and where are you innoculating against disease?

HEROES

4. EMPOWER A CULTURE BY TRAINING & INVOLVING YOUR HEROES

HEROES

The characters in your Storyboard, or Heroes, consist of every stakeholder from board members and executives to managers and employees. Heroes can be either your weakest link or your strongest line of defense. You get to decide which. Regular, engaging security awareness training of the specific people in charge of the business activity you define in steps one and five is not a waste of funds - it is the only way to put technology to use with minimal risk and maximum efficiency.

HEROES

What kind of Security Awareness Training do you provide your heroes? Who exactly needs to be trained and on what risks to protect these Stakes?

STAKES

5. PRIORITIZE ACTION BASED ON YOUR MOST CRITICAL BUSINESS ACTIVITIES

Your Stakes or critical business activities are the centerpiece and driving force of the Storyboard. These can be financial, operational, trade secrets, innovation, market expansion, relationships, etc. and can be internal or external to the organization. Sometimes the attackers goal is disruption or data manipulation rather than theft. To determine critical Stakes, the Storyboard team should interview leaders as well as consult annual reports, risk tolerance statements and company objectives. The number of critical activities that a company has, and therefore Storyboards, will vary by organization.

STAKES

What are the most important business activities in which you engage? Where are these activities most at risk? How could they fail in a way that damages the organization? Build a Cyberstakes Storyboard for every high-stakes activity that you provide.

SETTING

6. IDENTIFY HOW CURRENT SYSTEMS & PROCESSES PROTECT YOUR STAKES

SETTING

The Setting defines the systems that support your Stakes. The task here is to build a prioritized inventory of computer systems and the services, processes and functions that they provide for each Stake in question. This process is generally initiated by operational employees involved with the business activity, as they are familiar with the supporting software. The IT team(s) supporting these critical business systems should also be included as well as engineers responsible for any Industrial Control Systems connected to the activity.

SETTING

What computers, servers, cloud services, software, networking equipment, mobile devices, apps and industrial control systems support this key business activity? Which are the most critical to operations and profitability? Which are the most vulnerable to inside or outside attack? Inventory every system, including physical location.

ADVERSARIES

7. DETERMINE WHO IS OUT TO CONTROL YOUR STAKES AND WHY

ADVERSARIES

It is important and often difficult to determine who is targeting your Stakes, but the exercise is important nonetheless. Common Adversaries include: organized crime, unwitting insiders, competitors, nation-states, hacktivists, terrorists and lone hackers. Less common adversaries are customers, malicious insiders and 3rd-party vendors. Common motivations include: financial gain, espionage, blackmail, terrorism, operational control, reputation destruction, R&D or IP theft, social causes, hacker credibility, layoffs, political affiliations and cyber warfare. Look outside of your company for Adversaries that want to disrupt your products, services or bottom line.

ADVERSARIES

Who is out to get you? Who would benefit most from controlling your Stakes? Why?

ATTACK

8. ANTICIPATE THE MOST LIKELY FORMS OF ATTACK & LEARN FROM FAILURE

Outline all of the types of Attacks that could disrupt each high-stakes activity. Cyberattacks generally exploit vulnerabilities in computer systems, network connectivity, backup schemes, mobile devices and the humans that use them. Common Attack vectors include: malware, ransomware, zero-day exploits, social engineering, phishing, whaling, brute force hacking, physical theft, known vulnerabilities, insider exfiltration and many others.

ATTACK

What are the most likely forms of Attack? What would be required by the Adversary (knowledge, tools, physical access) to carry out this attack? What are the potential consequences of this type of Attack?

VICTORY/SEQUEL

9. DON'T FORGET THAT EVERY STORY HAS A SEQUEL

VICTORY/SEQUEL

Victory is fleeting in cyber risk. Adversaries and attacks are rarely linear and never really stop. You must be in this for the long game, not counting on one victory ending the war. Whether you are parallel processing each attack or addressing them by priority, you need to repeat Steps 1-9 for each high-Stakes business activity, Adversary and Attack mode. This forms the foundation of your Strategic Action Plan mentioned in Step 3.

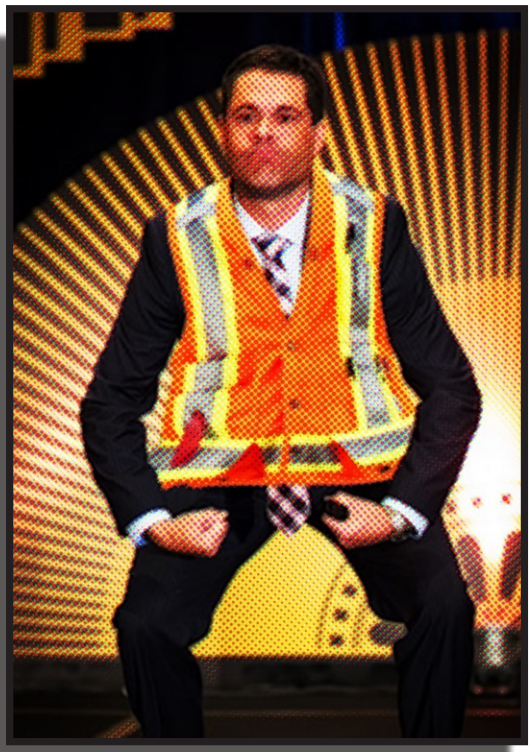
VICTORY/SEQUEL

What is the next most critical business activity that you provide? Return to Step 1 and repeat.

VICTORY/SEQUEL

The goal here is to build a Cyberstakes Strategy Board that maps out all of your key business activities and Action Plans, and then communicate it to all parties involved. Your Storyboards and Strategy Boards will constantly change and evolve as dynamic plans. By following these steps diligently and repeatedly, you will be able to change your cyber risk story.

JOHN'S BIO



John Sileo left hi-tech consulting and became an entrepreneur to reclaim his greatest priority – being present for his family. Six successful years, a thriving $2M business and two precious daughters later, he lost it all to cybercrime. Because the cybercriminal masked the crimes using John's identity, Sileo was held responsible for the felonies committed. The losses destroyed his company, decimated his finances and consumed two years as he fought to stay out of jail. And from these bitter circumstances, John made lemonade.

John Sileo is an award-winning author and highly sought-after cyber expert from 60 Minutes to the Pentagon, USA Today to Rachel Ray. His satisfied clients include a Who's Who of the Fortune 1000, Government, Associations and Small Business. The CEO of a Denver-based cyber think tank, an honors graduate from Harvard University and an inductee into the National Speakers Hall of Fame, John still values his remarkable wife and highly spirited daughters over all other successes.

JOIN THE CONVERSATION

linkedin.com/in/Sileo

fb.com/JohnDSileo

youtube.com/JohnSileo

John_Sileo

303•777•3221

john@sileo.com