Elevate Security

Fantastic Metrics

And Where to Find Them

By Masha Sedova, Co-Founder and Chief Product Officer, Elevate Security

Elevate Security

Going from security awareness to **security readiness** starts with measurable behavior change. This means relying on some fantastic **metrics**, and knowing where to find them.

When you're tasked with building your company's security awareness program, it's easy to dive right into the training content, and use training completion as the measure of success. But this misses the business-critical step of asking those classic questions:

What are you trying to drive awareness around?

How will you know what to train and build campaigns on?

Who needs training the most?

When do we know we've met our goals?

How should your company answer the above? Well, it's different for every organization, but ultimately it comes down to being able to measure your employees' security behaviors.

Basically, you need to start with metrics.

With a metrics-first approach, you can start with a baseline to benchmark current gaps in your security culture, and how, when or if those gaps close as your security awareness program goes on. And you'll have a much easier time communicating up to executives to show the value of your work. This is something I learned and implemented in my days working at Salesforce and that we now help companies address every day here at Elevate Security.

When you're able to show measurable impact to your employees' security behaviors, you'll be able to show that your program has matured beyond "security awareness' to what we call "security readiness." Security readiness means that your employees aren't a liability or a weak link. Instead, they're empowered with the training, rewards and reinforcement to be security superheroes, a front-line of defense against the 90% of incidents and losses that try to exploit human behaviors.

Elevate Security

In this guide, we'll show you how to leverage metrics to build a successful security behavior change program, including:

- What metrics to use for goals to measure how and when your employees' security behavior improve
- The systems and software your company may use where you can source those metrics
- How to verify or test the data from those sources

Typical goals of a security behavior change program

Phishing:
Reducing the click-through rate
Increase the reporting rate

Using Internet Safely:
Reduce the amount of unknown and malicious sites visited
Reduce the number of dangerous downloads on the network

Handling Sensitive Information:
Reduce the amount of sensitive information given over the phone
Reduce the amount of sensitive data stored outside of the network
Reduce the number of sensitive documents not shredded
Reduce data inappropriately stored (ie on local laptop)
Reduce sensitive data sent over email

Password Hygiene:
Increase the number of people who use a password manager
Reduce password reuse across sites

Social Media:
Reduce the amount of sensitive data posted on social media sites

Physical Risk:

Reduce the number of unauthorized badgze surfing attempts

Increase in the number of clean desks

Increase in the number of people who lock their screens when stepping away

Working Safely Outside the Office:

Increase in the number of people connecting via VPN

Increase in the number of privacy screens used

Decrease in the number of insecure Wifi connections used

Reduce the number of public conversations

Where to source and verify security behavior change metrics

	What does this mean?	Technology Sources for Data	How to test/verify?
Using the Internet Safely	Browsing to unknown/malicious sites, dangerous downloads, etc	• Proxies - Bluecoat, ZScaler, Websense • Endpoint - SentinelOne, Carbon Black, Cylance, Symantec, Trend	• These solutions, if they have an API and results are associated with a user and not a machine or IP will give very good insight into this behavior. • Phishing of employees
Handling Sensitive Information	Proper handling of sensitive data (storage/transit), social engineering	• Proxies - Bluecoat, ZScaler, Websense • DLP - Vontu	• These solutions, if they have an API and results are associated with a user and not a machine or IP will give very good insight into this behavior. • Social Engineering could be done through custom-built tools like phishing/vishing simulations.
Password Hygiene	Utilizing strong passwords on websites, password reuse	• Password Managers - LastPass, Keypass • Custom Built Browser Plugin	• Looking at exposed password sets and matching against employee names.
Using Social Media Safely	Posting information on social media sites which puts the individual or company at risk	• Zerofox	• Zerofox presented a tool they plan to open source on automating twitter phishing attacks. Could use this tool for testing click rate. • Create a profile that friends employees and asks for data
Protecting Mobile Devices and Information	Mobile device configuration and settings plus basic endpoint security	• Endpoint - Lookout, ESET, Trend, etc • MDM Vendors - Airwatch, MobileIron, Good, etc	• For endpoint malware solutions, if they have an API and results are associated with a user and not a machine or IP it will give very good insight into this behavior.
Protecting and Disposing of Data Securely	For individuals who have legitimate access, how do they handle the data once they move it to other devices?	• Proxies - Bluecoat, ZScaler, Websense • DLP - Vontu	• Aggregate pentest findings for insecure data storage
Protecting Against Physical Risk	Badge Surfing, not locking machines, clean desk		• Manual assessments of unlocked machines, badge surfing, and clean desk policy • Video reviews of a set of doors at the same time each week for a period of time. • Surveys
Working Safely Outside the Office	WiFi, physical security, connecting via VPN, public area conversations	These only detect bad outcomes, not bad behavior. • Proxies - Bluecoat, ZScaler, Websense • Endpoint - SentinelOne, Carbon Black, Cylance, Symantec, Trend	• Survey

TAKE THE NEXT STEP TOWARDS SECURITY READINESS

Get a demo of the Elevate Platform, which empowers your team to visualize and analyze your company's security posture by capturing all your security behavior metrics in one place.

Email hello@elevatesecurity.com to get started

About Masha Sedova

Masha Sedova is an industry-recognized people-security expert, speaker and trainer focused on engaging people to be key elements of secure organizations. She is the co-founder of Elevate Security, an innovative new approach to security awareness. Before Elevate, Masha was a security executive at Salesforce where she built and led the security engagement team focused on improving the security mindset of employees, partners, and customers. In addition, Masha is a member of the Board of Directors for the National Cyber Security Alliance and a regular presenter at conferences such as Blackhat, RSA, ISSA, Enigma, and SANS.

About Elevate Security

Elevate Security is the first fully integrated Security Behavior Platform. Elevate enables CISOs and security awareness practitioners to transform employees into security superheroes as a first line of defense against the 93% of security incidents that target human error. Customers across industries, from Autodesk to Clover, have seen employee detection and reporting of attacks improve by 5x or more. With offices in Berkeley, CA, and Montreal, Elevate is backed by Defy Partners, Costanoa Ventures, and is currently hiring. To learn more, please visit elevatesecurity.com.

Elevate Security