Tracking security awareness KPIs

Effective tools for measuring security awareness program impact, tracking workforce behavior & proving organizational value

infosecinstitute.com/iq/
Executive summary

Hackers have leveraged security vulnerabilities as early as the 1980s to break into networks and capture data. Since that time, attacks have increased in frequency, reach and sophistication. Organizations have answered this threat by investing in security technologies, but a look at recent headlines shows this effort is not enough. Using social engineering tactics like phishing, hackers have learned to circumvent security controls and access networks through unassuming, underprepared employees.

A comprehensive approach to information security is an organization's best defense against security threats. This includes investments in security technology and staff, security policy development and workforce security awareness training. But like all investments, we need to prove a positive return to management. In this paper, we review the value of security awareness training and suggest key performance indicators (KPIs) to help you demonstrate program value to stakeholders.

Table of contents

Security awareness training: 1
Assessing security awareness training program success with KPIs 2
Selecting effective security metrics 3
Nine security awareness KPIs to track program impact 4
Conclusion 5
About Infosec IQ 6
Security awareness training: A powerful risk mitigation tool

Security awareness training is a prerequisite for many international security standards and regulations, including ISO 27000 series and PCI DSS. However, an effective security awareness program also adds considerable value to your organization’s security strategy. End point users are the weakest link in the cybersecurity chain; the human element is often the primary cause of many severe data breaches through simple mistakes like downloading malware to clicking links in phishing emails. By teaching your workforce how to detect cyber threats, they will be better equipped to prevent data breaches at your organization.

According to Verizon’s 2018 Data Breach Investigations Report, human error led to 27 percent of data breaches in 2017. Other findings include:

» 43 percent of all breaches leveraged social attacks
» 93 percent of social incidents occurred due to phishing
» 28 percent of phishing breaches were targeted attacks
» 51 percent of all breaches included malware
» 66 percent of malware was installed through email attachments

Cyber criminals have humanized their hacking methods – and as the data shows, it’s working. By exploiting common drivers of human behavior like eagerness, distraction, curiosity and uncertainty, hackers can easily convince uninformed users to share sensitive data or install malware. With so many security risks stemming from human behavior, awareness training for your workforce can be an effective tool in the prevention, detection and early reporting of security breaches.

Like most investments, security awareness training is only as good as the results it generates. It’s important to objectively monitor the effectiveness and impact of your program through metric-based tracking. Before launching your program, establish program KPIs in collaboration with your organization’s stakeholders. Defining training program success – and what metrics you will use to define it – will align program objectives with business strategies. This will ensure continued support and funding for your future training program initiatives.
Assessing security awareness training program success with KPIs

Security awareness KPIs will help you measure the effectiveness of your training program, identify gaps and drive change. Select measurable, meaningful and easy-to-understand KPIs that align with the goals of the organization and legislation. All KPIs should be easy to implement and inexpensive to track – with a finite budget and resource pool, it’s important your management process is not burdensome.

Once KPIs are selected, define how to use them to create meaningful performance scorecards that tell a story. It’s helpful to define acceptable ranges for KPIs, as well as milestones to reach and “tripwires” to trigger action when needed. Some KPIs measure quantitative items (e.g., phishing rates); others can look at less tangible indicators like risk ratings and surveys.

There are three compelling reasons to track program impact with KPIs:

1. **You can’t manage what you cannot measure.**
   In order to better administer the security awareness program and justify its cost, find a good, objective method to verify its effectiveness. Measurable results prompt acceptance, support investments and justify change implementation when needed.

2. **Track workforce behavioral changes overtime.**
   KPIs can help demonstrate how the program is affecting user behavior. Program effectiveness can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid phishing attempts.

3. **Prove value from training.**
   Budget for training expenditures must be justified to management. Getting funding for security technology is relatively simple -- antivirus software is clearly effective in stakeholders’ minds -- but securing funding for security awareness training is often more challenging. Having an evaluation plan and KPIs in place prior to program launch will help gain management buy-in and financial support.

Select measurable, meaningful and easy-to-understand KPIs that align with the goals of the organization and legislation.
Getting started:

Selecting effective security metrics

Depending on your program's objective, your choice of KPIs will vary. As noted in the NIST publication Cyber Security Metrics and Measures, “effective security metrics identify weaknesses, determine trends to better utilize security resources and judge the success or failure of implemented security solutions.” Whatever KPIs you select, make sure they help you answer key questions, both from a program management perspective and from organizational stakeholders. These may include:

- Is your security awareness program reducing operation costs?
- How is your security awareness program helping mitigate security risks?
- How is your security awareness program changing workforce behavior?
Nine security awareness KPIs to track program impact

Once you’ve identified the questions your KPIs must address, it’s time to select your program KPIs. Here are nine indicators to help you evaluate and measure security awareness at your organization.

1. **Policy acknowledgment:** Every security awareness program should, at minimum, communicate security policy requirements to staff. Tracking employee policy acknowledgments will ensure your workforce is aware of the policy, and helps the organization meet compliance requirements.

2. **Phishing rate:** You can measure phishing rates through phishing simulation programs that track learners’ abilities to detect and avoid phishing emails. A reduction in phishing rate overtime proves increased awareness of security threats.

3. **Attack detection:** Track this metric by recording the amount of hacking attempts detected and reported to your security team. Some security awareness programs include an email plugin that allows your staff to report suspicious emails and attachments, which can help inform this KPI.

4. **Self-reported incidents:** A quick response to a security incident can greatly reduce damages from an attack. Your security awareness training should teach your workforce what to do if they downloaded a malicious file or clicked a phishing email. While the goal of your program should be to help the workforce avoid attacks altogether, this metric will prove you have safeguards in place in the event of a breach.

5. **Number of security breaches:** A reduction of breaches over time, especially those related to human error, is a good indicator of program success.

6. **Audit hits:** This is the number of items flagged for correction during a security audit. Periodic internal and external audits are a good way to evaluate your overall security strategy, including awareness training.

7. **Program participation rates:** Measuring program participation rates gives great insight on training quality and engagement. Simply delivering awareness training will “check the box” on a security audit, but will not help you determine workforce engagement. If your program participation rates are low, consider changing program content or delivery method to increase engagement – and effectiveness.

8. **Security health:** This KPI can be presented as an overall user behavior grade. To determine security health, pick a sample of your workforce and monitor their technology use. Tracking the number of security infections on their machines, unauthorized downloads or browsing activity can help gauge training retention. Assign weight to these behaviors to generate a meaningful security health score for monitoring changes over time.

9. **Cost of security breaches:** For this KPI, specifically track the cost of incidents caused by human error. Include related costs, such as those incurred through incident response (tech support, public relations, etc.) and lost productivity. This is an interesting metric that shows management a direct link between awareness and cost reduction.
Conclusion

Security awareness training KPIs can inform your program management process from development to evaluation. Selecting program KPIs that gauge program impact while linking outcomes to business objectives will help you secure and maintain support for ongoing training initiatives. Security needs change constantly, and so should your training program content. Having data-backed insights into your program’s effectiveness will allow you to make changes as needed to mitigate security risks across your entire organization.

Sources

1. Cyber Security Metrics and Measures, NIST
2. The Components of Top Security Awareness Programs, Infosec
3. The Role of Scorecards and Dashboards in Performance Management, ThomasNet
4. Infosec Book Excerpt: Security Metrics – Chapter 17, Infosec
5. 10 Tips to Embed Positive Information Security Behaviors in Employees, CIO
6. Security Awareness Metrics: Measure What Matters - Part 1, Native Intelligence
7. Measuring Security Awareness Program Results, SANS
8. Information Security Awareness Program – What is the Key to Make it a Success?, SecureReading
About Infosec IQ

Infosec IQ awareness and training empowers your employees with the knowledge and skills to stay cybersecure at work and home. With over 2,000 awareness and training resources, you’ll have everything you need to prepare employees to detect, report and defeat cybercrime. Every aspect of the platform can be customized and personalized to match your organization’s culture and employees’ learning styles. With Infosec IQ, you can:

- **Personalize** employee training with role-based modules in a variety of themes, styles and lengths to engage learners
- **Automate** training cadence and delivery to keep lessons relevant, challenging and fun — and save you time
- **Integrate** with your endpoint protection, LMS and SOC to streamline program management, reporting and attack response
- **Analyze** employee risk scores, learning outcomes and reported phishing threats to anticipate — and remediate — cyberthreats
- **Improve** your program with actionable dashboard data, helping you fill compliance training gaps and educate high-risk employees

Learn more at [infosecinstitute.com](http://infosecinstitute.com)