SANS SECURITY AWARENESS

Whitepaper

Managing Your Human Risk Starts with Identifying It

Achieve Data-Driven Results with Behavioral Risk Assessments

Written by **Lance Spitzner**, SANS Institute,
Director Research & Community

August 2022

Overview

Cybersecurity is no longer just about technology, it's also about people. People represent not only one of the biggest risks to organizations, but also one of the fastest-growing risks. According to the 2022 Verizon Data Breach Investigations Report (DBIR), over 80 percent of reported breaches in the last year involved a human element. Security awareness is part of—and an extension of—security teams that enable organizations to effectively manage and measure that risk.

Security teams often have different specialties to help manage different elements of risk. These specialties include vulnerability management, endpoint security, security operations centers (SOCs), and incident response teams. Every tool is another piece of the puzzle—and increasingly, these pieces are focusing more on the human side of risk.

How Do You Manage Human Risk?

Mature security awareness programs effectively manage human risk through a three-step strategic process:

1. Identify an organization's top human risks
2. Define the key behaviors that most effectively manage those risks
3. Communicate with, train, and engage the workforce to instill those key behaviors

To truly manage all elements of cyber risk, organizations need to focus not only on technology, but also on the human side of risk. This white paper explores how organizations can more effectively complete the first step of any mature awareness program: identifying your top human risks.

Where Does My Human Risk Exist?

One of the most common ways to start any risk management program is with a risk assessment. The purpose of a risk assessment is to inform decision makers of the identified threats that are relevant to their organization, the potential impact if these threats were to materialize, and likelihood that harm will occur.

The concept of risk assessments is not new, and there are numerous options and frameworks such as **NIST SP800-30** and **FAIR** from which to take guidance. An effective risk assessment requires using data to drive your decisions as much as possible. Far too often, risk decisions are based too much on emotion.

A common challenge with any risk assessment is getting a solid handle on three basic questions:

- What is your most sensitive data?
- Where is that data stored?
- How is that data processed?

And, as is becoming increasingly prudent, a fourth question:

- Who is accessing that data and how?

Remember, for most organizations, the goal is to secure sensitive data, so risk assessments often start with identifying what systems are handling your sensitive data and how. Adding a layer of human risk to your assessments is no different, except that instead of focusing solely on the systems that are handling your data and how, the aim is to identify who is handling your most sensitive data and how. One of the easiest ways to accomplish this step is to simply ask your workforce using a quick behavioral risk assessment.

Why Metrics?

Metrics enable us to better manage and illustrate what we are doing right and what we need to change or focus on more. Metrics are difficult in security, in part due to the difficulty of measuring the elements of risk. Security teams as well as GRC practitioners often are challenged to address the following risk measurement concepts:

- How do you put a quantitative value on threats when they come from a malicious, sentient actor who is always adapting and changing?
- How do you put a quantitative value on vulnerabilities if you don't know what all the vulnerabilities are?
- How do you put a value on impact when you don't know how much your customer database or reputation are worth?
- How do you measure something that is not happening?

What Should I Measure?

Now that we are diving into impact metrics, we'll next need to answer what should be measured. In many ways, that may be the wrong question. Instead, consider starting with the following steps:

- Measure what you care about, managing organizational risk
- Identify and prioritize your top risks
- Identify and prioritize the key behaviors that manage those risks
- Then measure those behaviors you have identified

How Much Should I Measure?

There are a couple of key concepts when it comes to metrics. First and foremost, focus on only the most useful metrics to you and your organization. Far too often, organizations create overwhelming metric dashboards for the sake of metrics. Keep it simple. Also, keep in mind that the value of metrics is often not found in a single snapshot in time, but rather, in the impact or change over time. This is especially true for leadership. The value of metrics is in demonstrating how your Security Awareness Program is moving the needle in managing human risk.

SANS Security Awareness Behavioral Risk Assessment™

Behavioral risk assessments are extremely powerful in helping you identify not only who is handling your most sensitive data, but also how they are handling it and which methods may be the riskiest. The resulting data and the recommended training plan ensure that you will provide the right training to the right people, ultimately reducing program costs and eliminating unnecessary training. Additionally, you can leverage this data for compliance purposes, as compliance is often driven by the type of data people handle.

At SANS, our work with global organizations to achieve data-driven result metrics for their security awareness programs has led us to recognize the need to quickly and efficiently identify the who, what, and where of data-handling risk. By leveraging an evaluation such as the SANS Security Awareness Behavioral Risk Assessment™, organizations can easily identify the top risks to focus on based on their unique set of weighting and risk scoring. This assessment is best leveraged as you plan your program, and then again after you've run the program, to quantify your human risk measurement results and identify which elements you should focus on next.

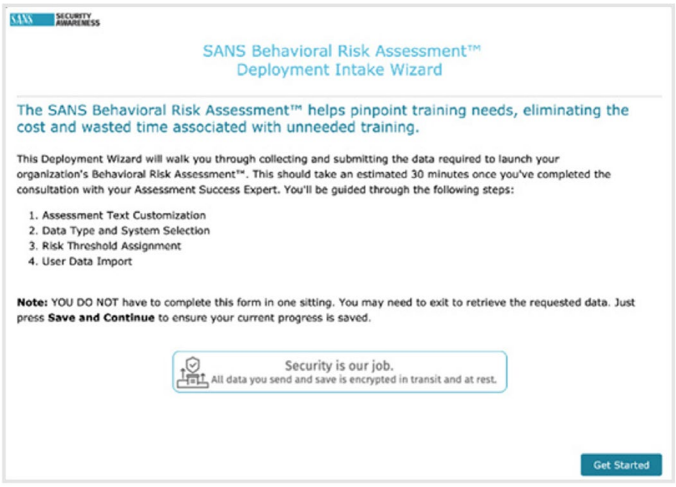
Getting Started

The SANS Security Awareness team will work with you to define the data types and systems specific to your organization. We help you customize and deploy the assessment and interpret reports within the system. Employees' participation is quick and accurate because the assessment is tailored to use non-technical language and terms they understand.

Once you've established your team of internal stakeholders—which typically include representatives from the Security, Information Technology (IT), Governance, Risk Management, Compliance (GRC), and Human Resources departments—you'll work with SANS to customize the assessment and build executive support. Some thoughts on achieving a successful cross-functional deployment can be found in the **Best Practices box at the end of this paper.**

A SANS Security Awareness team member will be with you every step of the way.

Quick and Easy Deployment



Guided by SANS client services experts, the consultive customization process prior to launch takes about 4–6 hours in total, including the stakeholder collaboration mentioned above. The risk model can be programmed with customized risk values for data, systems, individuals, organizations, and roles.

Using the assessment's Deployment Wizard, shown in the accompanying image, you can collect and submit the data required to launch your organization's behavioral risk assessment. You'll be guided through the following five steps:

1. Data Type and System Selection, Naming, and Description Customization
2. Customized Risk Thresholds Assignment
3. Assessment Text Customization
4. Organizational Reporting Groups
5. Training Assignment Configuration
6. User Import

The look and feel, language, and branding of the assessment can be modified, as can the entire lexicon and the names of all systems and data.

The average assessment takes 2–4 minutes for end users to complete.

A View of Results

Upon launch, users will select the types of data they access and the systems they use to access, store, process, and/or transmit each type of data. Once the assessment is launched, you'll receive access

to the filterable and customizable dashboard of your results and a Security Awareness Training Plan tailored to address the identified risk behaviors.

Below are screenshots of results taken from our SANS Security Awareness Behavioral Risk Assessment.

Figure 1 shows the utilization of different systems to process and store data types and the resulting risk associated with using each one. From this view you can quickly identify which organizational units are practicing which behaviors and the degree of risk associated with each one.

Figure 1: Data and System Risk

Other dashboards within the Behavioral Risk Assessment break down information by data classification levels, risk scores, and organizational behavior. Figure 2 shows the percentage of high, medium, and low risk behaviors by organizational unit.

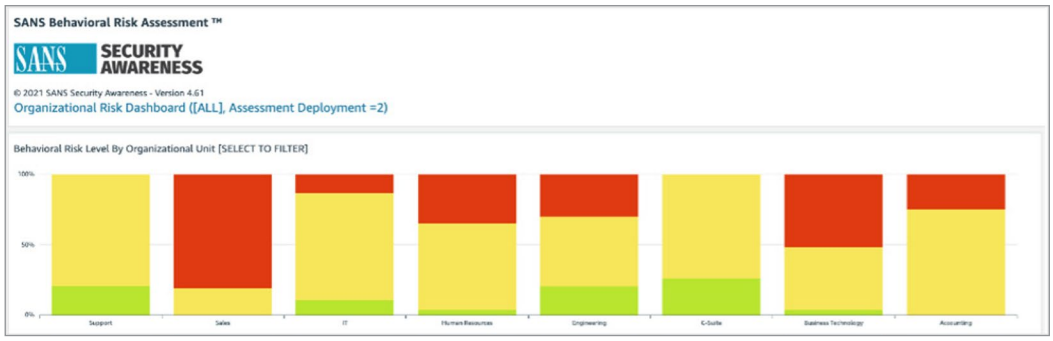


Figure 2: Risk by Organizational Unit

For example, your risk analysis can be taken further to identify not only your sensitive data, but also how that sensitive data is being used and the data that is at greatest risk. The heat map in Figure 3 enables you to quickly identify the greatest risk (red) as cardholder data being handled with email. These views help to better visualize which areas of your organizations are managing high levels of risk.

Using Data-Driven Results to Identify and Manage Risk

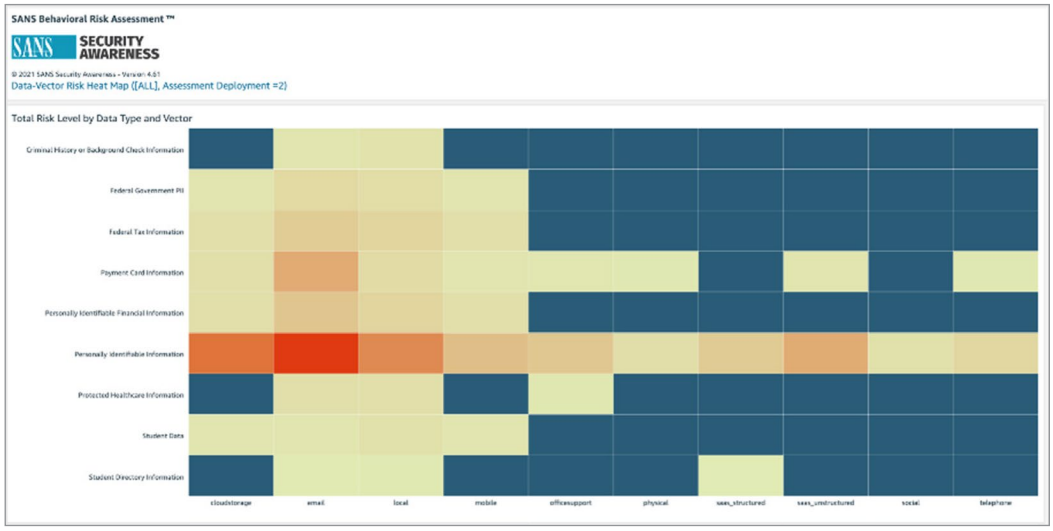


Figure 3: Data/System Heat Map

Results from the Behavioral Risk Assessment will help to identify a broad set of human risks to your data. These risk levels help you understand and prioritize how to respond. For example, behavioral data can indicate where security awareness training (see Figure 4) may be required, uncover shadow IT while identifying policy and technology gaps, expose any third-party risk, and even help prioritize how to respond by risk level. This unique, practical approach informs your program with actual data and allows for a calculated program response while shining a spotlight on the highest risk practices at your organization.

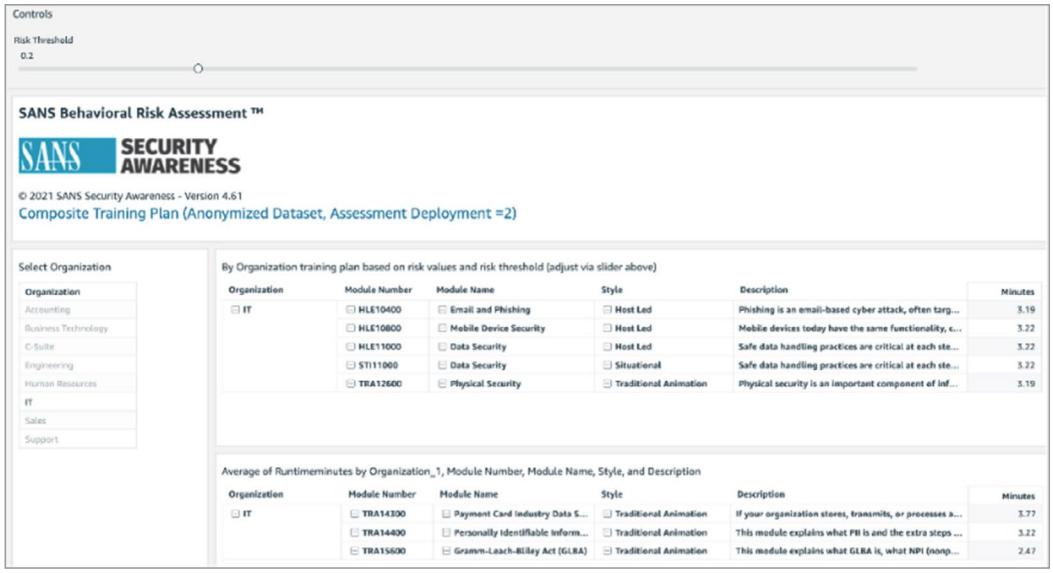


Figure 4: Risk/Compliance Based Training Plan

While the goal of cybersecurity is to generally manage information security risk to an acceptable level, the goal of a mature security awareness program is to manage the human risk to data and systems.

A key component to managing this risk is delivering the right training to the right people at the right time. To address these needs, the SANS Behavioral Risk Assessment Dashboard uses analytics of risk and compliance data to recommend the appropriate SANS Security Awareness Training content to be assigned to organizational units, teams, or divisions. SANS experts will work with you to optimize the training plan configuration based on your specific program goals.

ROI and Human Cyber Risk Reduction

How do we know if actual risk has been reduced? The Behavioral Risk Assessment is designed and licensed to be used regularly to chart the improvements made under the program and to define the next set of risks to address. Trend views of the data can be used to understand the impact your program is having on measured human risk and help you adjust your program to address emerging risks. Figure 5 shows the relationship between data handling risk level and frequency of activity; how often risky behaviors are being practiced at your organization.

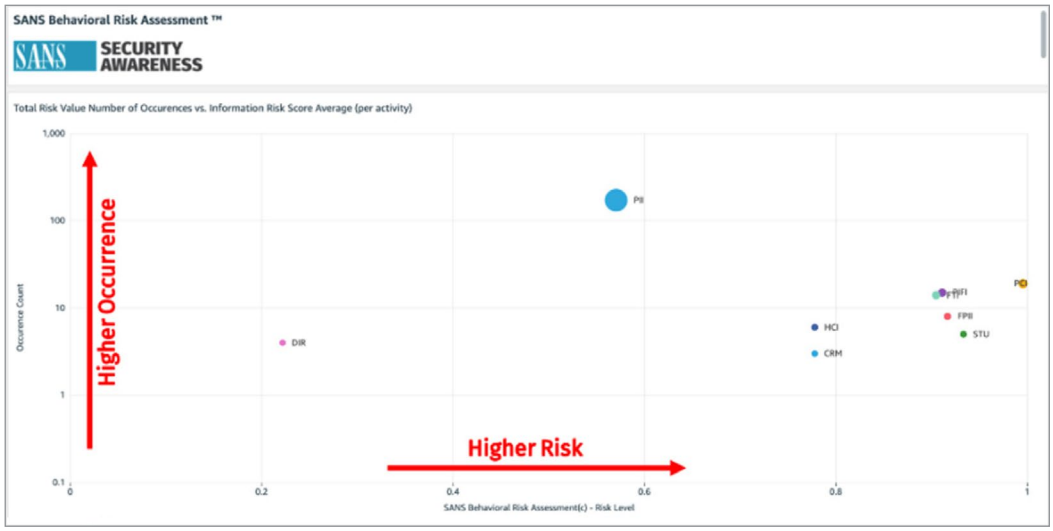


Figure 5: Risk Occurrence Plot

Aligning Strategic Metrics in Your Organization

Risk is likely already being measured and managed to one degree or another in many parts of your organization, ranging from the CISO and CFO to the GRC Department and the Board of Directors.

Tying your security awareness impact metrics to those risk metrics already being tracked will illustrate how your program supports the strategic goals of the Security Awareness Program and ultimately your organization's mission.

For example, consider how your Security Awareness Program is helping your CISO and ultimately your organization's mission with overall security metrics such as the:

- Number of incidents per month
- Reduction in costs due to incidents
- Average time to detect and respond to an incident
- Number of policy violations
- Number of compliance and audit violations

Conclusion

Your ability to leverage data to identify the top human risks to your organization will directly impact your ability to effectively manage those risks. The SANS Security Awareness Behavioral Risk

Assessment™ allows you to identify how information about risk is being handled at your organization. These insights will deeply inform risk management planning and support the development of a plan to allow you to more effectively manage human risk.

You can learn more about the SANS Security Awareness Behavioral Risk Assessment™ here.

Best Practices: Successfully Deploying Risk Assessments

A key element to managing human risk is to first identify, prioritize, and measure risks. To accomplish this, we need to interact with people and measure qualities such as their knowledge, attitudes, and beliefs regarding key security behaviors and company policies. In addition, we need to measure more quantitative elements such as what data employees are handling, how they are handling that data, and who they are sharing it with.

Tools such as knowledge and behavioral risk assessments are used to obtain this data. But since using these tools take up peoples' time, gaining leadership support is critical to the successful deployment of any assessment tool. Consider the following approaches for your organization:

- **Sell Human Risk:** Help your leadership better understand the "why" behind knowledge assessments and that cyber security is not just about technology but about people as well. The behaviors your employees exhibit and the policies they follow, especially when handling sensitive data, are key to securing your organization.
- **Involve Human Resources:** If you will be doing any type of assessment or survey, you may want to consider discussing it with HR first. HR staff are experts on employee surveys and assessments, and they are often the gate keepers in terms of administering them.
- **Keep It Short:** When it comes to assessing people, time is literally money. It would be great to ask all your employees 30–50 questions, but sometimes you are simply limited to as few as 3–5 questions. The key here is to start not by developing the questions to ask, but instead by identifying, documenting, and prioritizing what it is you want to know, then have that drive the questions you will ask.
- **Assess Privacy Impact:** Privacy concerns within the organization often present implementation challenges. In most cases, you can gain the insight you need without knowing an individual's name. Consider tracking results by role, department, and/or region. Asking general demographic questions such as someone's role, department, or how long they have been at the organization could yield the results needed.

About the Author

Lance Spitzner, the Director of Research & Community for the SANS Institute, has over 25 years of security experience in cyber threat research, security architecture and awareness, and training. He helped pioneer the fields of deception and cyber intelligence with his creation of honeynets and by founding the Honeynet Project. In addition, Lance has published three security books, consulted in over 25 countries, and helped over 350 organizations build security awareness and culture programs to manage their human risk. Lance is a frequent presenter and serial tweeter (**@lspitzner**), and he works on numerous community projects. Before information security, Lance served as an Armor Officer in the U.S. Army's Rapid Deployment Force. He earned his MBA from the University of Illinois.

About SANS Security Awareness

SANS Security Awareness provides organizations with a complete and comprehensive security awareness solution, enabling them to easily and effectively manage their human cybersecurity risk. With more than 1,300 organizations and 6.5 million people around the world utilizing SANS Security Awareness's globally relevant, expert-authored tools and training to enable individuals to shield their organization from attacks, as well as a fleet of savvy guides and resources.