WEBINAR SUMMARY

January 14, 2021

Mind Games: Using Data to Predict and Solve for Employee Risk

Masha Sedova, Co-founder, Elevate Security
Perry Carpenter, Chief Evangelist and Strategy Officer, KnowBe4

KEY TAKEAWAYS

- Human risk is one of the largest unsolved problems in security.
- Security performance and phishing resiliency are correlated with factors like geography, tenure, and training completion.
- To reduce security risks, organizations must incorporate motivation hacks into their employee interventions.
- Humans are wired for deception and social engineers exploit this fact.
- Scam artists use cognitive biases to hack and hijack people's minds.
- Education and healthy security habits are the only defense against social engineering.

in partnership with

KnowBe4
Human error. Conquered.

OVERVIEW

Employees' security decisions are the primary vector for enterprise security breaches and years of research have found that compliance-driven, one-size-fits-all strategies for security are ineffective.

Better approaches blend behavioral science with data analysis. New solutions include risk mapping that helps prioritize risk mitigation efforts, interventions that increase employee motivation to "do the right thing," and security programs that focus on social engineering and how the human mind functions.

CONTEXT

Masha Sedova and Perry Carpenter discussed why the industry's traditional approaches to reducing employee risk are ineffective and shared research-based practices to strengthen organizational security.

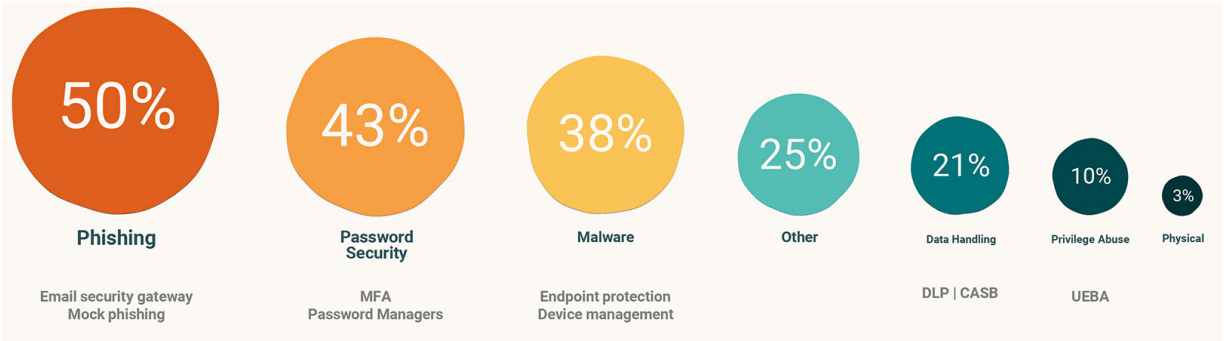
KEY TAKEAWAYS

Human risk is one of the largest unsolved problems in security.

The top reasons for data breaches and security incidents haven't changed in recent years. In response, security leaders have invested in technologies to mitigate these underlying attack vectors. Although that approach has worked to some extent, it hasn't been a silver bullet.

The reason that technology can't completely reduce security risks is because every attack vector has a human component. As long as human risk remains unaddressed, it will continue to be the soft underbelly of security.

Figure 1: Despite Significant Technology Investment, The Same Breaches Reoccur

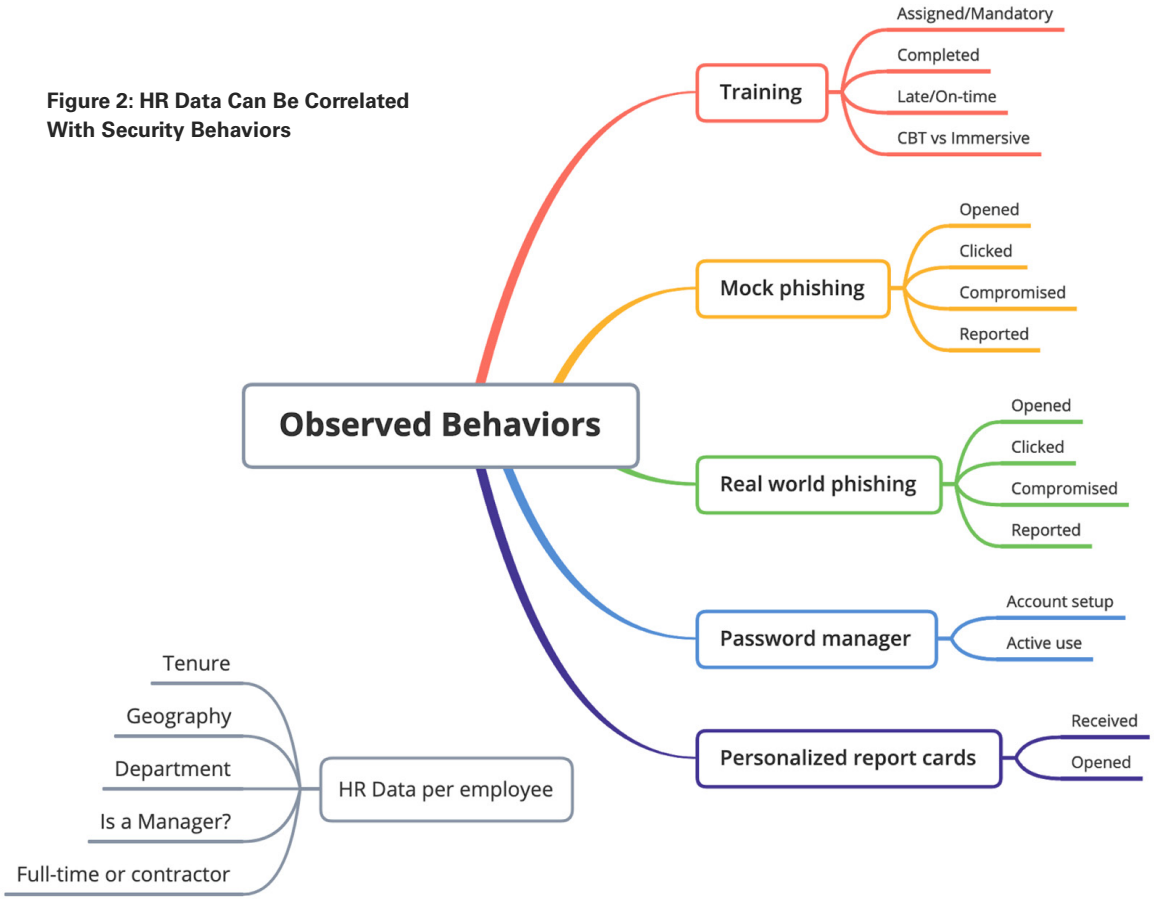


> There is a human component to every attack vector. As long as that remains unaddressed, unexplored, and unresolved, it will continue to be the soft underbelly of security.
>
> *Masha Sedova, Elevate Security*

Security performance and phishing resiliency are correlated with factors like geography, tenure, and training completion.

Elevate Security compiled a data set of over one million behavioral actions. These were gathered from more than 80,000 employees who were observed over an 18-month period.

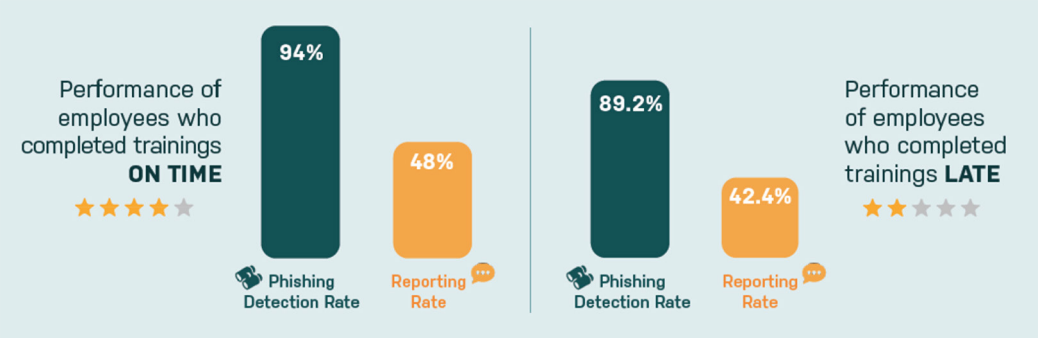
Figure 2: HR Data Can Be Correlated With Security Behaviors



This information revealed several predictors of security performance based on HR and behavioral data:

- **Geography is the strongest indicator of password manager usage, while tenure only slightly affects password manager utilization.** Employees in Asia Pacific who have been with the company longer than 1.3 years are least likely to use a password manager. Employees in the U.S. who have been with the company longer than 1.3 years are most likely to use a password manager.
- **Tenure is the strongest indicator of phishing resiliency.** Short-tenured contractors on large teams are most likely to fall for a phish, while employees in the U.S. who have been with the company more than 3 years but less than 16 are least likely to fall for a phish.
- **Late training completion signals poor security performance.** Late completion of security training was correlated with lower phishing detection and lower phishing email reporting rates.

Figure 3: On-Time Training Completion Is Linked with Higher Phishing Detection and Reporting Rates



> If you apply factors like geography, tenure, and being late for training, you get insights into which employees may need greater attention from the security team. It provides interesting information about where to look for employee risk in the organization.
>
> *Masha Sedova, Elevate Security*

To reduce security risks, organizations must incorporate motivation hacks into their employee interventions.

Dr. B.J. Fogg from Stanford University identified three elements required for behavior change: motivation, ability, and a reminder to take action. All three must exist at the same moment and in the right amounts to generate behavior change.

To increase employee motivation around security, organizations can use three "hacks":

1. Social proof. Social proof leverages the idea that humans strive to make decisions as efficiently as possible. To short circuit critical thinking, the human mind believes that if other people are doing something, it must be a good idea. Examples of social proof are online reviews or product recommendations based on the behavior of similar people.

   The key is to lead people toward things they already care about, like belonging to a social group. An example is a study showing that when people learned their Facebook friends were using an extra security setting, they were 1.36 times more likely to apply this setting to their Facebook accounts.

2. Gamification. Gamification incorporates game mechanics into non-game environments to improve engagement, motivation, and business results. Gamification is most effective when it includes five principles: autonomy, mastery, feedback, purpose, and social interaction. Loyalty programs, fitness trackers, and airline points programs all incorporate aspects of gamification. In the area of security, gamification is used in employee security strength ratings, leader boards that rank departments based on their security behaviors, and team or company-based security goals.

3. Positive reinforcement. This reinforces a behavior because a desirable outcome follows that behavior. Positive reinforcement is rarely used by security teams. Employees typically follow security programs to avoid some sort of penalty, such as getting locked out of a system. With phishing, for instance, positive reinforcement can be used to reward employees for identifying and reporting suspicious emails. By engaging in desirable behaviors, employees receive public recognition. Although both negative and positive reinforcement are effective, positive reinforcement creates a positive culture around desirable security behaviors.

Humans are wired for deception and social engineers exploit this fact.

To be human is to deceive and be deceived. Humans are born with the innate ability and desire to deceive others. The fundamental problem is that people can also be deceived themselves.

The root of deception is the mind's ability to filter, interpret, and present "reality." People must recognize that they don't see information clearly and don't process information perfectly. One person's reality can feel completely different from another's because they pre-processed information in a different way. Social engineers use filtering to deceive others.

> Deception is in our nature as humans. We are born with the innate ability and desire to put one over on others. The fundamental problem is that we are all master deceivers, but we are also very easily deceived.
>
> *Perry Carpenter, KnowBe4*

Scam artists use cognitive biases to hack and hijack people's minds.

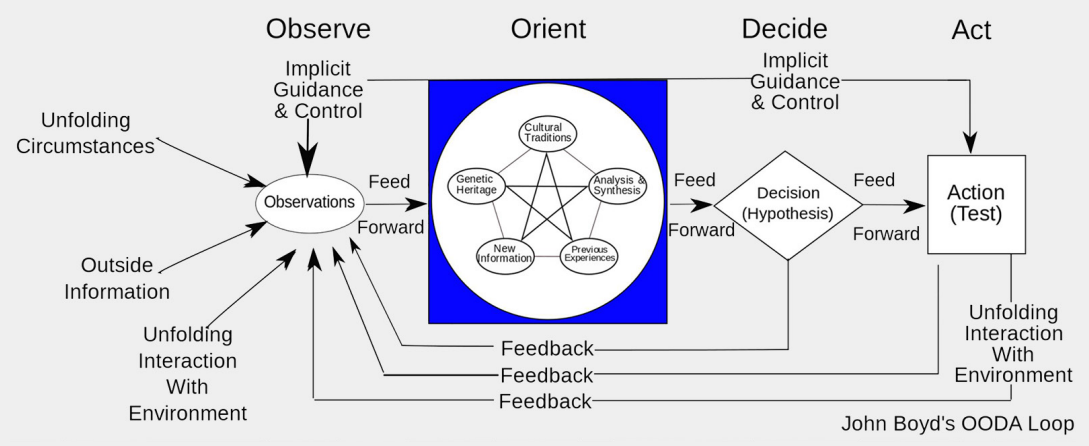
Humans rely on System 1 and System 2 thinking. System 1 thinking uses shortcuts to facilitate fast processing. About 95% of our thinking is governed by System 1. In contrast, System 2 thinking is slower and more reliable. It takes self-control, however, to stay in System 2 thinking as our minds are continually trying to return to System 1.

The shortcuts inherent in System 1 lead to cognitive biases and errors that underlie much of our thinking and all of our assumptions. Bad actors can easily exploit cognitive biases that lead to social, political, racial, and societal divisions.

The OODA (Observe, Orient, Decide, Act) Loop is a framework that illustrates how attackers manipulate others. Humans experience the OODA Loop several times per second. We observe input around us, orient ourselves based on our preconceptions of the world, decide what to do, and then take action.

Attackers are constantly trying to insert themselves into the observe and orient stages of the loop to manipulate people to act in certain ways. They poison information that people observe or they take advantage of the ways that people contextualize or orient themselves around the information.

Figure 4: The OODA Loop



Education and healthy security habits are the only defense against social engineering.

Three recommendations that organizations and individuals can use to avoid social engineering schemes are:

1. Watch for exploitation and manipulation. To lure people into scams, attackers often focus on greed, urgency, curiosity, fear, self-interest, or helpfulness.
2. Look for disinformation. Disinformation weaponizes information and makes people believe things that fit an established narrative. It's a byproduct of cognitive bias and System 1 thinking.
3. Beware of the "4Ds." Russia's "4D" offensive strategy is characterized by dismissing an opponent's claims or allegations that are inconvenient, distorting events to serve political purposes, distracting from one's own activities, and dismaying those who might otherwise oppose one's goals so they don't investigate and stop what's going on.

> In our society, we need a better understanding of the world we live in and how it can be exploited. Education, preparation, and healthy security habits are the only defense for a world where social engineering and our thoughts can be hacked and hijacked.
>
> *Perry Carpenter, KnowBe4*

BIOGRAPHIES

Masha Sedova

Co-founder, Elevate Security

Masha Sedova is an award-winning 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, the leader in human risk management software helping security leaders in enterprises measure, communicate, and reduce human risk to keep their companies safe from cyber threats.

Before Elevate Security, Masha Sedova was a security executive at Salesforce where she built and led the security engagement team focused on improving the security among employees, partners, and customers. In addition, Sedova has been a member of the board of directors for the National Cyber Security Alliance and regular presenter at conferences such as Black Hat, RSA, ISSA, Enigma, and SANS.

Perry Carpenter

Chief Evangelist and Strategy Officer, KnowBe4

Perry Carpenter currently serves as Chief Evangelist and Strategy Officer for KnowBe4, the world's most popular security awareness and simulated phishing platform.

Previously, Carpenter led security awareness, security culture management, and anti-phishing behavior management research at Gartner Research, in addition to covering areas of IAM strategy, CISO program management mentoring, and technology service provider success strategies. With a long career as a security professional and researcher, Carpenter has broad experience in North America and Europe, providing security consulting and advisory services for many of the best-known global brands.

Carpenter holds a Master of Science in Information Assurance (MSIA) from Norwich University in Vermont and is a Certified Chief Information Security Officer (C|CISO).