SecurityAdvisor

A CISO's Guide: Mitigating the Human Risk Factor

Understanding what makes us tick and click —strategies for reducing preventable cyber breaches

Understanding What Makes Us Tick and Click

Human error is undoubtedly the biggest risk factor to a sound security posture for any organization. 90% of all data breaches result from human error and yet many organizations don't have a program in place to protect the human attack surface. Security teams deploy several technologies to protect their attack vectors (network, endpoints, email, web, cloud apps, etc.) but what about the human attack surface?

Despite efforts to educate and train employees to spot phishing attempts, an all-too-common horror continues. An employee in the finance department receives an email from the CEO, asking him to immediately pay a vendor invoice. The email includes an attachment of the invoice, along with the CEO's email signature. With the urgency communicated in the email, the employee pays the invoice and moves on with their day. Unfortunately, the CEO's email was spoofed.

People, no matter their tech savviness, are often duped by these scams because of their familiarity and immediacy factors.

The FBI's 2020 Internet Crime Report includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion.[1]

Cybersecurity is not just a technological challenge, but increasingly a social and behavioral one. The top reasons cyber breaches happen point to human actions, according to Willis Towers Watson.[2] From mistakenly disclosing account information to falling for phishing attacks, an organization's data can leak through legitimate channels and compromise its security. This social engineering easily bypasses technology barriers.

The biggest issue is that hackers have become increasingly savvy at launching specialized attacks that target specific employees by tapping into their fears, hopes, and biases to get access to their data. With a better understanding of how hackers are duping employees, companies can identify potential biases, deliver training that actually changes behaviors, and cut down on security incidents.

The FBI recorded an 61% increase in BEC complaints in 2020, amounting to **$1.8 billion in losses** to organizations.

Understanding Cognitive Bias

Behavioral economics studies the effects of psychological, cognitive, emotional, cultural, and social factors on the decisions of individuals and institutions.[3] Behavioral economics came of age in 1970 thanks to the work of Israeli social scientists, Nobel Prize winning economist, Daniel Kahneman and Amos Tversky.[4] The understanding of cognitive psychology was revolutionized by their discovery of emotional biases. Kahneman and Tversky found significant evidence that humans, in certain circumstances, show a systematic pattern of deviation from the norm or rational judgment.

Five decades later, their research is helping companies understand why they're seeing their own employees easily fall for cyber breaches. **Every day, hackers use specific cognitive biases to repeatedly target employees, according to research by SecurityAdvisor.** To truly understand how hackers operate, the SecurityAdvisor study assessed more than 500,000 data points from real-world situations to see how hackers leverage human cognitive biases to trick end users. Each data point was mapped to one or more of Kahneman and Tversky's discovered biases.

Every day, hackers use specific cognitive biases to repeatedly target employees.

Top 9 Cognitive Biases Used by Hackers

Hackers tap into human cognitive biases, such as anchoring and representative heuristics, to sway their decisions based on irrelevant or misleading information and based on false or generalized categorization. Employees are enticed to click on fraudulent links or share sensitive company data through fake coupons or fake messages from 'team managers.'

Hyperbolic discounting:
"Here's a free coupon"

Authority bias:
"Hey its your CEO"

Halo effect:
"Message from Apple"

Habit:
"Here is your daily delivery report"

Optimism:
"A 30% pay hike"

Loss aversion:
"Act now to save your credit score"

Recency:
"Avoid coronavirus"

Curiosity:
"Here is your secret offer - click here"

Ostrich:
"You have 800 visruses"

Security Leaders Must Break Down Employees' Cognitive Biases

Cybercriminals purposefully use fear, authority/hierarchy, and familiarity tactics to trick end-users into clicking links or opening viral attachments. Phishing emails are highly effective today because workers have been groomed to have an immediate response to them, particularly remote workers.

Phishing scams leverage **authority bias** where people tend to attribute greater accuracy to the opinion of an authoritative figure. If an employee receives a request from their CEO to share a password or pay an invoice, for example, they would be more likely to not question that request before fulfilling it.

Hackers use "**recency bias**" and "**halo effect bias**" to send employees emails with COVID-19 tips or tax returns from what looks like legitimate global organizations, such as the World Health Organization (WHO) and IRS. These messages may have malicious content as embedded links or attachments.

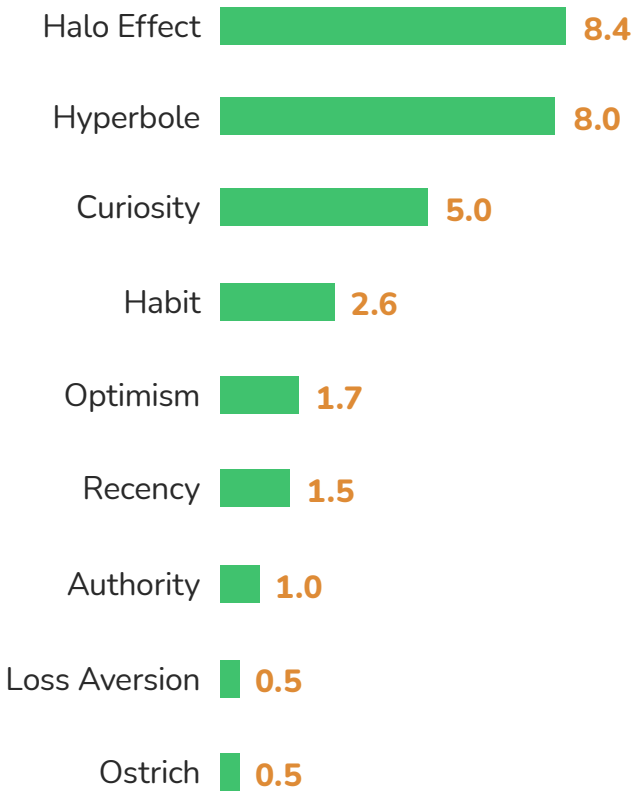
Stoking our fears of compliance and security with the "**ostrich effect bias**," hackers send emails or pop-up notifications to employees, alerting them of a violation or viruses on their machine, and then offer a simple fix by clicking on a link. Many employees tend to postpone a patch deployment or update reminder from the IT team, so a message like this can trigger unintended consequences despite "good" intentions.

Loss aversion attacks prey on an individual's tendency to prefer avoiding losses to acquiring equivalent gains. An example of this bias in action can include acting on an outstanding payment to avoid late fees.

The impact of these biases on the business is defined by frequency and by severity. How frequently the bias is used is a strong indicator of the probability of the event occurring. Most people have received some type of phishing email based on the halo and hyperbolic biases. Given the frequency of these types of phishing emails, there is a high likelihood that employees will fall prey to it.

The severity impact relies on human fears as the employee grants higher authority in some form to do much harm. Granting access to their computer or transferring money in an unconventional way to comply with an urgent request may not be frequent, relatively speaking, but are often targeted. **The loss to the organization is potentially more damaging with these infrequent but severe attacks.**

Relative usage of cognitive biases by hackers



Nudging Toward a Secure World

Human biases are part of human nature, but that doesn't mean organizations can't learn from cognitive psychology and counteract these biases.[4] The work of Nobel Prize winner behavioral economist Richard Thaler, from the University of Chicago, shows that **decision architecture and human behavior can be influenced by 'subtle nudges**.' Based on indirect encouragement and enablement, the nudge theory offers curated choices that encourage people to make positive and helpful decisions.[5] This reshapes existing behaviors and counteracts innate human cognitive bias.

Nudge theory is now being used very effectively in cybersecurity to combat behavioral biases and help organizations obtain better defense against evolving security attacks. Humans learn and respond to in-the-moment reminders about behaving securely. One of the most common and best examples is the use of a password strength meter. As someone chooses a password, the longer and more complex it becomes, the more a bar fills up or a sad face turns into a smiley face.

6 Steps for a Cyber Immune Culture

Across the organization, people need to understand the fundamentals of making the most secure cyber decisions and what's expected from them in complying with security policies. Cybersecurity awareness training introduces the workforce to the organization's security policies, the most prevalent cyber threats, best practices for behaving securely, and how to reach someone for help with cybersecurity matters.

A comprehensive, personalized employee cyber engagement program, including education, training and assessment can be a game-changer.

1. Educate the entire organization on cybersecurity basics and roles.
2. Provide frequent and just-in-time training.
3. Customize training to specific role requirements.
4. Do not overdo phishing simulations.
5. Use AI and data analysis for a surgical and targeted approach for high-risk users.
6. Measure and report the results.

Organizations need to make their employees stronger cybersecurity advocates and weed out the bad habits that negatively impact the organization's cyber posture.

Many companies deliver security training as part of their new employee orientation with sessions lasting 2-4 hours. Annual refreshers are then required to remind the workforce of the expectations. But there are challenges with this approach. Employees find it boring and have short attention spans. Knowledge retention rates drop by more than 50 percent when training is more than two minutes. With traditional security awareness training, too much time passes between reminders, and companies risk a return to old habits and biases. Instead, **SecurityAdvisor recommends coaching employees through short, relevant messages**.

A Cornell study[6] showed that people are more motivated and more likely to adopt a new behavior when given small tasks and immediate small rewards. This is the same in cybersecurity. **A key enabler for the cyber immune culture is micro learning.** For better retention of the training, the content needs to be engaging, relevant, quick and frequent.

Knowledge retention rates drop by more than 50 percent when training is more than two minutes.

Next Gen Security for the Human Attack Vector

SecurityAdvisor analyzed malware sources across seven multinational firms and discovered that 5-10 percent of users account for more than 90 percent of malware infections. It's important to identify these high-risk users, and then provide them with specific guidance to reduce their infection rates.

SecurityAdvisor's patented platform delivers contextual educational content to workers during 'teachable moments' to quantifiably improve organizational security. The solution leverages analytics and AI to identify the riskiest users. The AI engine learns which approach works best for an organization, department, and user. This enables personalized, surgical delivery of relevant education.

5-10 percent of users account for more than 90 percent of malware infections.

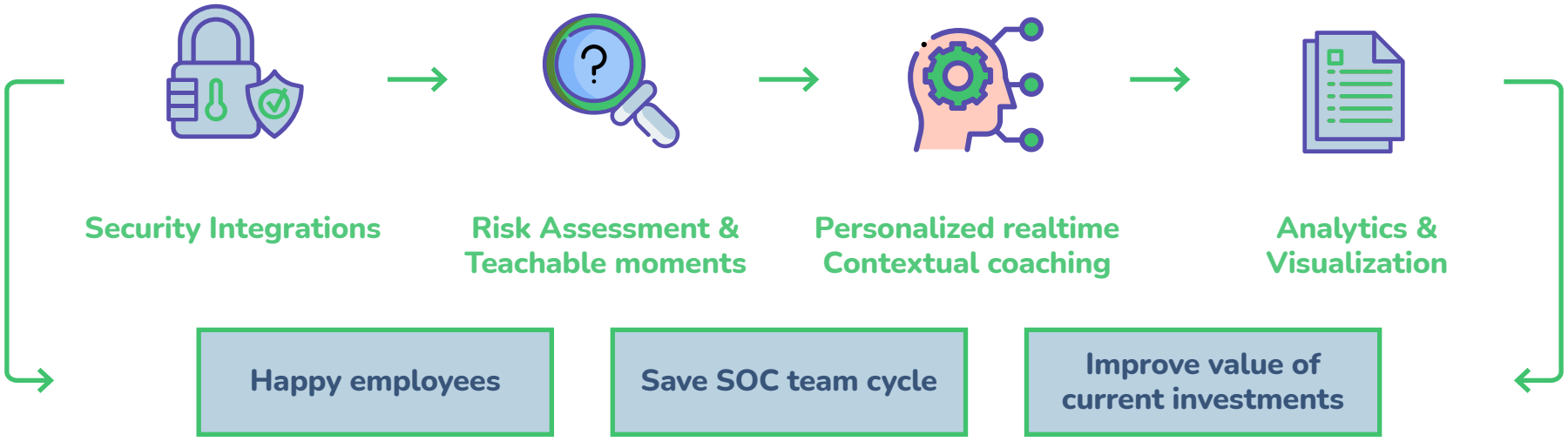
Source: SecurityAdvisor malware analysis from seven multinational firms

Our approach is helping global enterprises:

- Reduce overall security incidents by 70%
- Reduce email phishing attacks by more than 50%
- Lower endpoint malware detections by more than 90%
- Cut web violations in half
- Decrease removable media incidents by more than 90%

Source: SecurityAdvisor malware analysis from seven multinational firms

People are the first line of cybersecurity defense for organizations and must be prioritized. Cybercriminals use worker's innate brain function to trick them into performing risky behaviors. Focusing on the human element of your broader cybersecurity strategy is the only way to effectively combat sophisticated phishing and social engineering techniques. By providing real-time, personalized microlearning moments that directly correlate to an individual's behavior, businesses are able to educate their users more easily and reinforce good behaviors.



Methodology

SecurityAdvisor's analysis of over 500,000 emails that were either phishing emails or spam emails. The analysis used seven anonymized datasets collected by SecurityAdvisor. The analysis was done in seven spreadsheets. In each data set, pivot tables were run, and the subjects used by hackers were sorted. The subject that occurred the most was at the top and the subject that occurred the least was at the bottom. From there, the ten subjects that occurred the most in that sheet were mapped to a specific cognitive bias. This was repeated for each of the seven data sets. This way, over 500,000 emails were reduced to 70 data points. Knowing the frequency of occurrence of each of the 70 data points allowed us to sum up the frequency of occurrence for each cognitive bias and identify the most common cognitive biases leveraged by hackers.

About SecurityAdvisor

Founded in 2018, SecurityAdvisor provides the only real-time and personalized security awareness platform that delivers a measurable reduction in security incidents. The company's patented platform integrates easily with existing security infrastructure to deliver personalized coaching for each employee, teaching them how to identify and remediate cyberattacks and help security teams better understand the human element of their organization's security posture.

Learn more securityadvisor.io

Citations

1. FBI Internet Crimes Report 2020, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
2. Cyber Risk Culture Survey." Willis Towers Watson, 2018, www.willistowerswatson.com/en-US/Solutions/products/cyber-risk-culture-survey
3. The Rise of Behavioral Economics and Its Influence on Organizations, Harvard Business Review, Oct. 10, 2017. https://hbr.org/2017/10/the-rise-of-behavioral-economics-and-its-influence-on-organizations
4. Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science (New Series), 185, 1124–1131.
5. Hochma, Tomer. "Cognitive Biases: The Ultimate List of Human Irrational Decisions." HumanHow, 17 May 2018, http://humanhow.com/list-of-cognitive-biases-with-examples/
6. Hansen, P., & Jespersen, A. (2013). Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy. European Journal of Risk Regulation, 4(1), 3-28. doi:10.1017/S1867299X00002762
7. Woolley, K., & Fishbach, A. (2018). It's about time: Earlier rewards increase intrinsic motivation. Journal of Personality and Social Psychology, 114(6), 877–890.
8. Robin, Lily, et al. The Urban Institute, 2020, The Los Angeles Community Safety Partnership: 2019 Assessment, http://www.urban.org/sites/default/files/publication/101827/the_los_angeles_community_safety_partnership_2019_assessment.pdf